Creating Trust in
the Digital Society

utimaco®

u.trust

LAN Crypt

Produktversion: 13.0.1
Stand: Februar 2026

Inhaltsverzeichnis

Überblick

1.1 Was ist u.trust LAN Crypt?

u.trust LAN Crypt schützt vertrauliche Daten durch Dateiverschlüsselung. Es wurde entwickelt, um den vertraulichen Austausch von Daten zwischen Benutzern innerhalb von Berechtigungsgruppen in großen Organisationen zu ermöglichen. In diesem Fall können verschlüsselte Dateien sowohl lokal auf der Festplatte des Anwenders liegen als auch auf Wechselmedien oder Netzwerklaufwerken sowie in der Cloud gespeichert sein.

Alle Ver- und Entschlüsselungsvorgänge von Dateien des Benutzers erfolgen durch *u.trust LAN Crypt* automatisch und transparent. So werden Dateien, die einer Verschlüsselungsregel unterliegen, automatisch bei ihrer Erstellung oder Speicherung verschlüsselt bzw. beim Öffnen bzw. Lesen entschlüsselt, ohne dass der Benutzer dies wahrnimmt. Diese Prozesse erfolgen mithilfe eines Filtertreibers, der sich in das Dateisystem des Betriebssystems (z. B. Windows oder macOS) eines Rechners integriert.

Wie funktioniert der *u.trust LAN Crypt* Dateifiltertreiber? Ähnlich einem Virenscanner, erkennt der *u.trust LAN Crypt* Dateifiltertreiber, auf welche Dateien zugegriffen werden soll, und führt dabei jeweils die gewünschte Ver- oder Entschlüsselung durch. Jedes Mal, wenn ein Benutzer eine Datei in einen verschlüsselten Ordner kopiert oder verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt und jedes Mal, wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Ordner liest, wird sie in verschlüsselter Form übertragen und erst auf dessen lokalen Computer entschlüsselt. Bevor sie wieder in den verschlüsselten Ordner zurückgelegt wird, erfolgt wiederum auf dem lokalen Computer des Benutzers die Verschlüsselung der Datei.

Verschlüsselte Dateien sind nicht an einen einzelnen Benutzer „gebunden“. Alle Benutzer, die den hierfür erforderlichen Schlüssel besitzen, dürfen auf eine verschlüsselte Datei zugreifen. Dies erlaubt einem Security Officer (SO) das Erzeugen von logischen Benutzergruppen, die gemeinsam mit verschlüsselten Dateien arbeiten können. Dieser Vorgang kann mit einer Art Schlüsselbund, wie er im täglichen Leben verwendet wird, verglichen werden: *u.trust LAN Crypt* stattet Benutzer und Benutzergruppen mit einem Schlüsselbund aus, dessen Schlüssel für verschiedene Türen oder Safes verwendet werden können. Die Anzahl der Schlüssel, die ein Benutzer erhält, lässt sich dabei beliebig variieren.

Nicht berechtigte Benutzer können eventuell auf verschlüsselte Dateien zugreifen (jedoch nur von Arbeitsstationen ohne *u.trust LAN Crypt*). Sie sind jedoch ohne entsprechende *u.trust LAN Crypt*-Berechtigung nicht in der Lage, diese zu lesen. Auf diese Weise bleibt die Datei immer geschützt, auch wenn im Dateisystem selbst kein Zugriffsschutz definiert ist, das Netzwerk angegriffen wird oder die Mitarbeiter sich nicht an die Sicherheitsrichtlinien der Organisation halten. *u.trust LAN Crypt* ist das Produkt Ihrer Wahl, wenn es darum geht, geistiges Eigentum in Dateiform vor unberechtigtem Zugriff in einem LAN, auf Dateiservern, auf lokalen Festplatten, auf mobilen Datenträgern oder in der Cloud zu schützen.

Welche Dateien und Ordner durch *u.trust LAN Crypt* geschützt werden sollen, legt ein Security Officer (SO) zentral durch eine oder mehrere Verschlüsselungsrichtlinien fest. Um beispielsweise die Verschlüsselung aller Word-Dokumente sicherzustellen, definiert der Security Officer eine Verschlüsselungsregel für Dateien mit der Erweiterung **.docx* und weist dieser Regel einen Schlüssel zu. Sobald diese Regel über eine Richtliniendatei (Profildatei) auf die Clientrechner mithilfe der *u.trust LAN Crypt* Administration ausgerollt ist, werden fortan sämtliche Word-Dokumente verschlüsselt, und zwar unabhängig davon, wo sie sich befinden. Es lassen sich zudem auch mehrere Verschlüsselungsregeln zu einem Verschlüsselungsprofil kombinieren.

Die u. a. Tabelle veranschaulicht, wie Sie beispielsweise drei unterschiedliche Verschlüsselungsregeln für ein Verschlüsselungsprofil kombinieren können:

Regel	Schlüssel	Beschreibung
*.docx	Schlüssel1	Verschlüsselt alle Word-Dokumente mit „Schlüssel1“, unabhängig davon, an welchem Ort sich diese befinden.
D:\Daten*.*	Schlüssel2	Verschlüsselt alle Dateien im angegebenen Ordner mit „Schlüssel2“.
\\Server1\Share1\Personal*.xlsx	Schlüssel3	Verschlüsselt alle Excel-Dateien unter dem angegebenen Pfad des File-Servers mit „Schlüssel3“.

u.trust LAN Crypt erlaubt die Definition beliebig komplexer Regeln, sodass der Security Officer sicherstellen kann, dass nur die gewünschten Daten an den tatsächlich gewünschten Speicherorten verschlüsselt werden. Das Ausrollen von Regeln erfolgt über Profildateien (siehe „Erzeugen (Bereitstellen) von Profildateien“), welche auf einem File-Server oder im Netlogon-Verzeichnis eines Windows Domänencontrollers über die *u.trust LAN Crypt* Admin-Konsole abgelegt werden können. Per Mausklick erzeugt ein Security Officer für jeden Benutzer dessen eigene individuelle Profildatei. In dieser sind alle Schlüssel und Regeln zusammengefasst, die für diesen Benutzer fortan gelten.

Für die Erzeugung und Verwaltung der Profildateien nutzt der Security Officer die grafische Benutzeroberfläche der *u.trust LAN Crypt-Administration*. Diese bedient sich wiederum der *Microsoft Management Konsole (MMC*) als Schnittstelle. Snap-Ins stellen dem Security Officer Werkzeuge zur Verfügung, die ihn bei seiner Arbeit unterstützen.

Die Profildateien werden mithilfe von digitalen Zertifikaten für jeden einzelnen Benutzer geschützt. So sind u. a. alle in dieser Datei enthaltenen Schlüssel mit dem öffentlichen Schlüssel des Zertifikates des jeweiligen Benutzers verschlüsselt, sodass nur der jeweils berechtigte Benutzer, der für das verwendete Zertifikat auch den privaten Schlüssel besitzt, diese Datei über die *u.trust LAN Crypt*-Clientanwendung öffnen kann. Hierbei kann eine bereits in der Organisation vorhandene **P**ublic **K**ey **I**nfrastructure (PKI) zum Einsatz kommen. Alternativ kann der Security Officer auf die Möglichkeit zurückgreifen, die Zertifikate durch *u.trust LAN Crypt* selbst zu erzeugen.

Die Speicherung der Administrationsdaten von *u.trust LAN Crypt* erfolgt in einer SQL-Datenbank. In dieser SQL-Datenbank werden wichtige Datensätze und vor allem die Schlüssel verschlüsselt gespeichert. Durch den Einsatz einer von der Systemadministration unabhängigen Datenbank, lässt sich eine strikte Trennung der Sicherheits- gegenüber der Systemadministration realisieren. Darüber hinaus bietet *u.trust LAN Crypt* die Möglichkeit zur Konfiguration unterschiedlicher Security Officer-Rollen, deren Rechte sich je nach Anforderung wiederum beliebig einschränken lassen.

Lediglich ein Master Security Officer (MSO) verfügt stets über sämtliche Rechte. Ein Master Security Officer ist zudem in der Lage, individuelle Aufgaben und Rechte zur Administration von *u.trust LAN Crypt* an weitere Security Officer zu delegieren und so eine Administrationshierarchie zu schaffen, die der Organisationsform jedes Unternehmens gerecht wird.

1.2 Schutz von Daten durch u.trust LAN Crypt

u.trust LAN Crypt garantiert, dass sensible Dateien auf File-Servern, Cloudspeichern und Arbeitsstationen verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da Ver- und Entschlüsselungsvorgänge im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Daher muss hierfür beispielsweise auf einem File-Server keine spezielle Sicherheitssoftware installiert werden.

Die Profildateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden.

Damit ein Benutzer auf seiner Arbeitsstation Dateien mit *u.trust LAN Crypt* ver- und entschlüsseln kann, muss er in der Lage sein, auf seine Profildatei zugreifen zu können. Dies erfolgt durch eine Netzwerkfreigabe für den Speicherort, an dem sich die Profildatei befindet. Die sensiblen Inhalte der Profildatei sind verschlüsselt und durch ein Zertifikat vor nicht autorisierter Verwendung geschützt. Um sie verwenden zu können, muss der Benutzer den privaten Schlüssel seines Zertifikats besitzen und das Passwort kennen.

Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen transparent und weitgehend ohne die Notwendigkeit von Benutzerinteraktionen ab.

u.trust LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen durch die Definition unterschiedlicher Regeln auf Ordner- und Dateiebene. Die Sammlung dieser Regeln, Attribute und Schlüssel ergibt das Verschlüsselungsprofil für den Benutzer. Das persönliche Zertifikat und der dazugehörende private Schlüssel bieten wiederum durch sichere Verschlüsselungsverfahren hohen Schutz für die Profildatei, in der das Verschlüsselungsprofil gespeichert ist.

Alle *u.trust LAN Crypt* Benutzer, die in ihrer Profildatei dieselben Verschlüsselungsregeln gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Die Benutzer müssen sich daher weder um die Verschlüsselung noch um den Schlüsselaustausch kümmern. Sie benötigen nur den Zugriff auf die eigene Profildatei. Ist diese Voraussetzung erfüllt, werden die Dateien der Benutzer transparent ver- bzw. entschlüsselt, sobald sie geöffnet bzw. geschlossen werden.

Durch die Verteilung der Verschlüsselungsprofile mithilfe von Profildateien können alle Organisationsformen abgebildet werden: von einem zentralen LAN-Modell, in dem die Benutzer zentral administriert werden, bis hin zu einem verteilten Modell, bei dem die Benutzer nur Notebooks einsetzen.

u.trust LAN Crypt unterstützt neben Windows auch macOS sowie darüber hinaus für mobile Geräte auch Android und iOS.

Hinweis: Auch im normalen Betrieb lagert Windows meist Teile des Arbeitsspeichers auf die Festplatte aus. In manchen Fällen, etwa bei einem Absturz bzw. bei sog. "Blue Screens", kann sogar der gesamte Speicherinhalt auf die Festplatte geschrieben werden. Dadurch könnten sensitive Informationen, die sonst nur im Hauptspeicher verfügbar sind (wie z. B. die Inhalte geöffneter Dokumente), auf der Festplatte in einer Datei gespeichert sein. Eine Festplatten-verschlüsselung (wie beispielsweise mit *Utimaco DiskEncrypt*) gewährleistet, dass der Inhalt dieser oftmals sensitiven Daten in jedem Fall verschlüsselt auf der Festplatte gespeichert und somit gegen Ausspähung optimal geschützt ist. Aus diesem Grund wird der Einsatz einer Festplattenverschlüsselung als wichtiger Basis-Schutz und als sinnvolle Ergänzung beim Einsatz von *u.trust LAN Crypt* empfohlen.

u.trust LAN Crypt Administration und Windows Administration

Die Verwaltung der Verschlüsselungsprofile und die Konfiguration von *u.trust LAN Crypt* erfolgt auf einem eigenen Administrationsrechner. Um eine klare Unterscheidung zwischen der Windows Administration und der Administration von *u.trust LAN Crypt* zu erreichen, muss die Rolle eines Security Officers eingerichtet werden. Der Security Officer legt durch die Definition der Verschlüsselungsprofile in Profildateien fest, welche verschlüsselten Daten in welchen Ordnern abzulegen sind und wer auf diese Daten Zugriff hat. Nach der Erzeugung der Profildateien auf dem Administrationsrechner müssen diese an die Benutzer verteilt werden.

Zur Administration von *u.trust LAN Crypt* wird ein Windows-Standardmechanismus, die *Microsoft Management Konsole (MMC)*, verwendet. Die Benutzeroberfläche der *u.trust LAN Crypt* Administration besteht aus Snap-Ins für die MMC. Die *u.trust LAN Crypt* Administration speichert die meisten administrierbaren Objekte (Benutzerdaten, Schlüssel, Verschlüsselungspfade, etc.) in einer eigenen SQL-Datenbank.

Die Verwendung des Datenbankkonzepts anstelle von ausschließlich Windows-Mechanismen (z. B. Active Directory) hat vor allem zwei Vorteile:

- Systemadministration und Security-Administration können streng getrennt werden. Die Verwendung einer eigenen Datenbank macht *u.trust LAN Crypt* unabhängig von der Systemadministration. Die Schlüssel in der *u.trust LAN Crypt* Administrationsdatenbank sind verschlüsselt und dadurch vor unberechtigtem Zugriff geschützt. Zusätzlich verhindert die Datenbank, dass unbeabsichtigt Änderungen vorgenommen werden (z. B., dass ein Systemadministrator versehentlich ein benötigtes Sicherheitsobjekt löscht).

- Andererseits ist es oft nicht erwünscht, dass Personen, die keine Systemadministratoren sind, die Systemkonfiguration ändern können. Es liegt auf der Hand, dass es problematisch ist, Schreibrechte bei der Systemadministration zu delegieren. Auch aus dieser Sicht ist es sehr sinnvoll, die spezifischen Daten von *u.trust LAN Crypt* in einer separaten Datenbank geschützt zu speichern.

Um den bestmöglichen Schutz zu bieten, sind die *u.trust LAN Crypt* Funktionen in zwei Bereiche gegliedert:

- ***u.trust LAN Crypt* Benutzerfunktionen**

  Die *u.trust LAN Crypt* Benutzerfunktionen enthalten die Ver- und Entschlüsselungsregeln für Dateien. Diese Informationen befinden sich in einer geschützten Profildatei und sind zur täglichen Arbeit mit *u.trust LAN Crypt* notwendig. Sobald ein Benutzer seine Verschlüsselungsregeln geladen hat, werden die Dateien transparent ver- bzw. entschlüsselt. Es ist ansonsten kein weiterer Benutzereingriff mehr notwendig. Zusätzlich bietet *u.trust LAN Crypt* einige Anzeigefunktionen, die es dem Benutzer ermöglichen, sich „seine“ Verschlüsselungsregeln und seine ihm zur Verfügung gestellten Schlüssel anzeigen zu lassen.

- ***u.trust LAN Crypt* Security Officer Funktionen**

  Die *u.trust LAN Crypt* Administration bietet Funktionen, die einem Security Officer vorbehalten sind. Verschlüsselungsregeln können nur dann administriert werden, wenn man im Besitz eines Security Officer-Zertifikats ist und auch die hierfür erforderlichen Rechte hat. Nur dann ist es möglich, beispielsweise neue Verschlüsselungsprofile zu erzeugen oder bestehende zu verwalten.

Beide Komponenten lassen sich getrennt installieren.

Hinweis: Wenn Sie beide *u.trust LAN Crypt* Komponenten auf demselben Computer installieren, müssen diese unbedingt von der gleichen Version sein.

1.3 Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten Ordnern oder auf Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie von einer Benutzeranwendung (wie z. B. MS Office) geöffnet werden. Beim Speichern der Datei wird diese automatisch wieder verschlüsselt geschrieben bzw. erzeugt.

- Alle Dateien, für die eine Verschlüsselungsregel besteht, werden automatisch verschlüsselt.
- Werden Dateien in einen verschlüsselten Ordner verschoben oder kopiert, werden sie gemäß der für diesen Ordner definierten Verschlüsselungsregel verschlüsselt. Zudem ist es möglich, verschiedene Verschlüsselungsregeln für individuelle Dateierweiterungen oder -namen festzulegen, die sich in ein und demselben Ordner befinden. Die Verschlüsselung ist grundsätzlich nicht von Ordnern abhängig, sondern immer von den Verschlüsselungsregeln!

- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem die bisherige Verschlüsselungsregel nicht mehr gilt, bleiben die Dateien dennoch verschlüsselt, da die *persistente Verschlüsselung* standardmäßig aktiviert ist.
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem nicht mehr die bisherige Verschlüsselungsregel gilt, sondern eine andere, werden die betreffenden Dateien gemäß der neuen Verschlüsselungsregel verschlüsselt.
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, für den eine Ausnahme- oder Ignorieren-Regel gilt, werden die betreffenden Dateien gemäß der neuen Regel entschlüsselt.
- *Transparente Verschlüsselung* betrifft alle Arbeiten mit Dateien. Der Benutzer bemerkt nur wenig von den Ver- bzw. Entschlüsselungsvorgängen, da alle Prozesse automatisch im Hintergrund ablaufen.
- Über die **Persistente Verschlüsselung** kann verhindert werden, dass ein Benutzer ungewollt Dateien entschlüsselt, wenn er diese in einen Ordner kopiert oder verschiebt, für den keine *LAN Crypt* Regeln bestehen.

1.3.1 Zugriff auf verschlüsselte Daten

Ist der Benutzer nicht im Besitz des passenden Schlüssels, darf er nicht auf die verschlüsselten Dateien in einem Ordner zugreifen. Er kann dort solche verschlüsselten Dateien weder lesen, kopieren, verschieben, umbenennen noch löschen.

Verfügt der Benutzer über den Schlüssel, mit dem die Dateien verschlüsselt sind, kann er, auch wenn in seinem Verschlüsselungsprofil keine Verschlüsselungsregel auf diese Dateien verweist, diese Dateien jederzeit öffnen und mit ihnen arbeiten.

1.3.2 Ordner umbenennen oder verschieben

u.trust LAN Crypt führt aus Performance-Gründen beim Verschieben ganzer Ordnerstrukturen über den Windows Explorer keine Änderung des Verschlüsselungsstatus durch. Das bedeutet, dass es beim Verschieben eines ganzen Ordners zu keiner Ver- oder Entschlüsselung kommt.

Hinweis: Das gilt jedoch nur, wenn für den neuen Speicherort keine Verschlüsselungsregel besteht. Besteht eine solche jedoch, werden die Dateien nach der geltenden Verschlüsselungsregel des neuen Speicherortes verschlüsselt.

Waren die Dateien verschlüsselt, bleiben sie unter dem neuen Ordnernamen bzw. am neuen Speicherort verschlüsselt. Besitzt der Benutzer den dazugehörigen Schlüssel, kann er wie gewohnt mit diesen Dateien arbeiten.

Sicheres Verschieben: *u.trust LAN Crypt* ermöglicht zudem das sichere Verschieben von Dateien und Ordnern. Dabei werden die Dateien auch entsprechend der geltenden

Verschlüsselungsregeln bei Bedarf ver-, ent- bzw. umgeschlüsselt. Die Quelldateien werden nach dem Verschieben sicher gelöscht.

Diese Funktion steht über den Eintrag **Sicheres Verschieben** im Windows Explorer Kontextmenü zur Verfügung. Über einen Dialog kann dann ausgewählt werden, an welchen Ort die Dateien verschoben werden sollen.

1.3.3 Explizite Entschlüsselung von Dateien

Wenn eine Datei entschlüsselt werden soll, muss diese Datei nur an einen Ort oder in einen Ordner kopiert oder verschoben werden, für den keine Verschlüsselungsregel besteht. Sie wird dann automatisch entschlüsselt.

Das gilt allerdings nur unter der Bedingung, dass

- der Benutzer sein Verschlüsselungsprofil geladen hat,
- dieser über den dazugehörigen Schlüssel verfügt,
- für den neuen Ablageort keine Verschlüsselungsregel besteht,
- die Persistente Verschlüsselung deaktiviert ist.

Hinweis: Wenn Sie über den dazugehörigen Schlüssel verfügen, lässt sich eine Datei auch durch Kopieren oder Verschieben in einen Ordner entschlüsseln, für den eine Ausnahme- oder Ignorieren-Regel besteht.

1.3.4 Löschen verschlüsselter Dateien - Windows Papierkorb

Wenn Ihr Verschlüsselungsprofil geladen ist, können Sie jede verschlüsselte Datei löschen, für die Sie einen Schlüssel besitzen.

Hinweis: Im Grunde genommen handelt es sich beim Löschen von Dateien um ein Verschieben von Dateien in den Windows Papierkorb. Um den höchsten Sicherheitsstandard zu gewährleisten, bleiben die von *u.trust LAN Crypt* verschlüsselten Dateien auch im Papierkorb verschlüsselt. Um den Papierkorb zu leeren, ist kein Schlüssel notwendig.

1.3.5 Von einer Verschlüsselung ausgenommene Dateien und Ordner

Folgende Dateien und Ordner sind standardmäßig von einer Verschlüsselung automatisch ausgenommen (auch wenn für sie eine Verschlüsselungsregel definiert wurde):

- Dateien im Installationsverzeichnis von *u.trust LAN Crypt*.
- Dateien in den Ordnern *Programme* und *Programme (x86).*
- Dateien im Installationsordner von Windows.
- Dateien im Ordner *Windows.old.*
- Richtliniendatei-Cache.

  Der Ablageort kann über die *u.trust LAN Crypt* Konfiguration mithilfe einer Gruppenrichtlinie (GPO) spezifiziert werden und wird in der *u.trust LAN Crypt* Client-Anwendung über den Dialog **Client-Status** im Reiter **Profil** angezeigt.
- Stammverzeichnis des Systemlaufwerks. Unterordner werden nicht ausgenommen.
- Indizierte Speicherorte (search-ms).
- Dateien in Ordnern, die in *u.trust LAN Crypt* mit einer Ausnahme- ‚Ignorieren- oder Bypass-Regel definiert sind.

1.3.6 Persistente Verschlüsselung

Dateien bleiben durch *u.trust LAN Crypt* normalerweise nur so lange verschlüsselt, wie sie einer Verschlüsselungsrichtlinie unterliegen. Dateien würden somit entschlüsselt werden, wenn sie beispielsweise in einen Ordner kopiert oder bewegt werden, für den keine Verschlüsselungsregel gilt.

Wenn Sie nicht möchten, dass unerwünschte Klartextkopien von verschlüsselten Dateien erstellt werden, kann dies die **Persistente Verschlüsselung** verhindern. Mit der **Persistenten Verschlüsselung** können Sie somit sicherstellen, dass verschlüsselte Dateien nicht entschlüsselt werden, wenn sie verschoben oder kopiert werden.

Security Officer bzw. Systemadministratoren können dieses Verhalten in der *u.trust LAN Crypt* Konfiguration über eine Gruppenrichtlinie (GPO) in Windows deaktivieren. Standardmäßig ist diese Funktion in *u.trust LAN Crypt* bereits aktiviert. Wird die **Persistente Verschlüsselung** deaktiviert, so werden von verschlüsselten Dateien Klartextkopien erstellt, wenn sie an einen Speicherort kopiert/verschoben werden, für den keine Verschlüsselungsregel gilt.

Für die **Persistente Verschlüsselung** gelten folgende Regeln:

- Der *u.trust LAN Crypt* Treiber behält nur den Namen der Datei ohne Pfadinformationen. Zum Vergleich kann nur dieser Name benutzt werden. Es werden somit nur Situationen erfasst, in denen Quell- und Zieldatei einen identischen Namen haben. Wird die Datei während des Kopiervorgangs umbenannt, betrachtet *u.trust LAN Crypt* die resultierende Datei als eine „andere“, neue Datei. Sie unterliegt in solch einem Fall nicht der persistenten Verschlüsselung und wird unverschlüsselt angelegt.

- Dies gilt auch, wenn ein Benutzer eine verschlüsselte Datei durch **Speichern unter** an einen Ort speichert, für den keine Verschlüsselungsregel gilt. Das Ergebnis ist dann ebenfalls eine Klartextdatei.
- Informationen zu Dateien werden nur für eine begrenzte Zeit beibehalten. Dauert der Kopiervorgang zu lange (länger als 15 Sekunden), wird die resultierende Datei als andere, unabhängige Datei betrachtet. Sie unterliegt dann nicht mehr der persistenten Verschlüsselung.

1.3.6.1 Persistente Verschlüsselung und Verschlüsselungsregeln

Wie zuvor beschrieben, versucht die **Persistente Verschlüsselung** sicherzustellen, dass eine verschlüsselte Datei ihren Verschlüsselungsstatus aufrechterhält (d. h. mit dem ursprünglichen Verschlüsselungsschlüssel weiterhin verschlüsselt bleibt), wenn die Datei in einen Ordner kopiert oder verschoben wird, für den keine Verschlüsselungsregel gilt. Wird die Datei jedoch an einen Speicherort kopiert oder verschoben, für den eine andere Verschlüsselungsregel gilt, hat diese Verschlüsselungsregel eine höhere Priorität als die **Persistente Verschlüsselung**. Die Datei wird in diesem Fall mit dem in dieser Verschlüsselungsrichtlinie definierten Schlüssel und Algorithmus umgeschlüsselt.

1.3.6.2 Persistente Verschlüsselung und Ignorieren-Regeln

Eine **Ignorieren-Regel** (siehe „Ignorierenregel für diesen Pfad“) hat eine höhere Priorität als die **Persistente Verschlüsselung**. Verschlüsselte Dateien, die in einen Ordner kopiert werden, für den eine Ignorieren-Regel gilt, werden entschlüsselt, d. h. im Klartext gespeichert!

Die **Ignorieren-Regel** wird hauptsächlich für Dateien benutzt, auf die sehr häufig zugegriffen wird und bei denen kein bestimmter Grund für eine Verschlüsselung oder einen besonderen Schutz vorliegt. Dadurch lässt sich die System-Leistung steigern.

Hinweis: Für Dateien, die einer **Ignorieren-Regel** unterliegen, besteht kein Zugriffsschutz.

1.3.6.3 Persistente Verschlüsselung und Ausnahmeregeln

Eine **Ausnahmeregel** (siehe „Von Verschlüsselung ausschließen“) hat eine höhere Priorität als die **Persistente Verschlüsselung**. Verschlüsselte Dateien, die in einen Ordner kopiert werden, für den eine Ausnahmeregel gilt, werden entschlüsselt, d. h. im Klartext gespeichert!

Hinweis: Für Dateien, die einer **Ausnahmeregel** unterliegen, besteht weiterhin der Zugriffsschutz.

Hinweis: Befinden sich verschlüsselte Dateien in Ordnern, für die eine **Ausnahmeregel** gilt, können Benutzer, die im Besitz des hierfür erforderlichen Schlüssels sind, diese entschlüsseln. Eine erneute Verschlüsselung von Dateien in solchen Ordnern ist jedoch nicht möglich.

1.3.6.4 Persistente Verschlüsselung und Bypass-Regeln

Eine **Bypass-Regel** (siehe „Bypass-Regel setzen“) hat eine höhere Priorität als die **Persistente Verschlüsselung**. Verschlüsselte Dateien, die in einen Ordner kopiert werden, für den eine Bypass-Regel gilt, werden entschlüsselt, d. h. im Klartext gespeichert!

Hinweis: Für Dateien, die einer **Bypass-Regel** unterliegen, besteht kein Zugriffsschutz.

1.3.7 Einschränkungen bei der persistenten Verschlüsselung

Aus technischen Gründen gelten für die persistente Verschlüsselung einige Einschränkungen. Das tatsächliche Ergebnis der persistenten Verschlüsselung erfüllt unter Umständen nicht immer die Erwartungen der Benutzer. In den folgenden Szenarien kann dies der Fall sein:

Dateien, die unverschlüsselt bleiben sollten, sind verschlüsselt

- **Klartext-Dateien werden an mehrere Speicherorte kopiert und verschlüsselt, obwohl nur für einen dieser Speicherorte eine Verschlüsselungsregel besteht.**

  Wenn eine Klartextdatei gleichzeitig an mehrere Speicherorte kopiert wird, von denen für einen dieser Speicherorte eine Verschlüsselungsregel gilt, werden die anderen Kopien dieser Datei unter Umständen auch verschlüsselt, obwohl die ursprüngliche Datei nicht verschlüsselt ist. Wenn die Datei zum ersten Mal an einen verschlüsselten Speicherort kopiert wird, wird die Datei zur internen Liste des Treibers hinzugefügt. Wenn dann die zweite Kopie an einem anderen Speicherort erstellt wird, findet der Treiber von *u.trust LAN Crypt* den Dateinamen in seiner Liste und verschlüsselt daher auch die zweite Kopie.

- **Kurz nach dem Zugriff auf eine verschlüsselte Datei wird eine Datei mit dem gleichen Namen erstellt.**

  Wird kurz nach dem Öffnen einer Datei (d. h. beim Zugriff auf eine Datei) eine weitere Datei mit dem gleichen Namen erstellt, wird die neu erstellte Datei mit dem gleichen Schlüssel wie die zuerst geöffnete Datei verschlüsselt.

  Hinweis: Das gilt nur dann, wenn für das Lesen der verschlüsselten Datei und das Erstellen einer neuen Datei die gleiche Anwendung / der gleiche Thread verwendet wird.

  Typischer Anwendungsfall: Rechtsklicken Sie im Windows Explorer auf einen Ordner mit einer Verschlüsselungsregel und wählen Sie **Neu > Neues Textdokument.** Rechtsklicken Sie dann sofort in einen Ordner ohne Verschlüsselungsregel und wählen Sie abermals **Neu > Neues Textdokument**. Die zweite Datei wird dann ebenfalls verschlüsselt.

Dateien werden nicht verschlüsselt

- **Von einer Datei werden mehrere Kopien angelegt**

  Werden Kopien von einer verschlüsselten Datei im gleichen Ordner wie die ursprüngliche Datei erstellt, so werden diese Kopien nicht verschlüsselt. Da die erstellten Kopien unterschiedliche Dateinamen haben (zum Beispiel doc.txt im Gegensatz zu doc - Kopie.txt), schlägt der Abgleich des Dateinamens fehl. Die Dateien werden daher nicht im Rahmen der persistenten Verschlüsselung verschlüsselt.

1.3.8 Client-API und Verschlüsselungs-Tags für DLP-Produkte

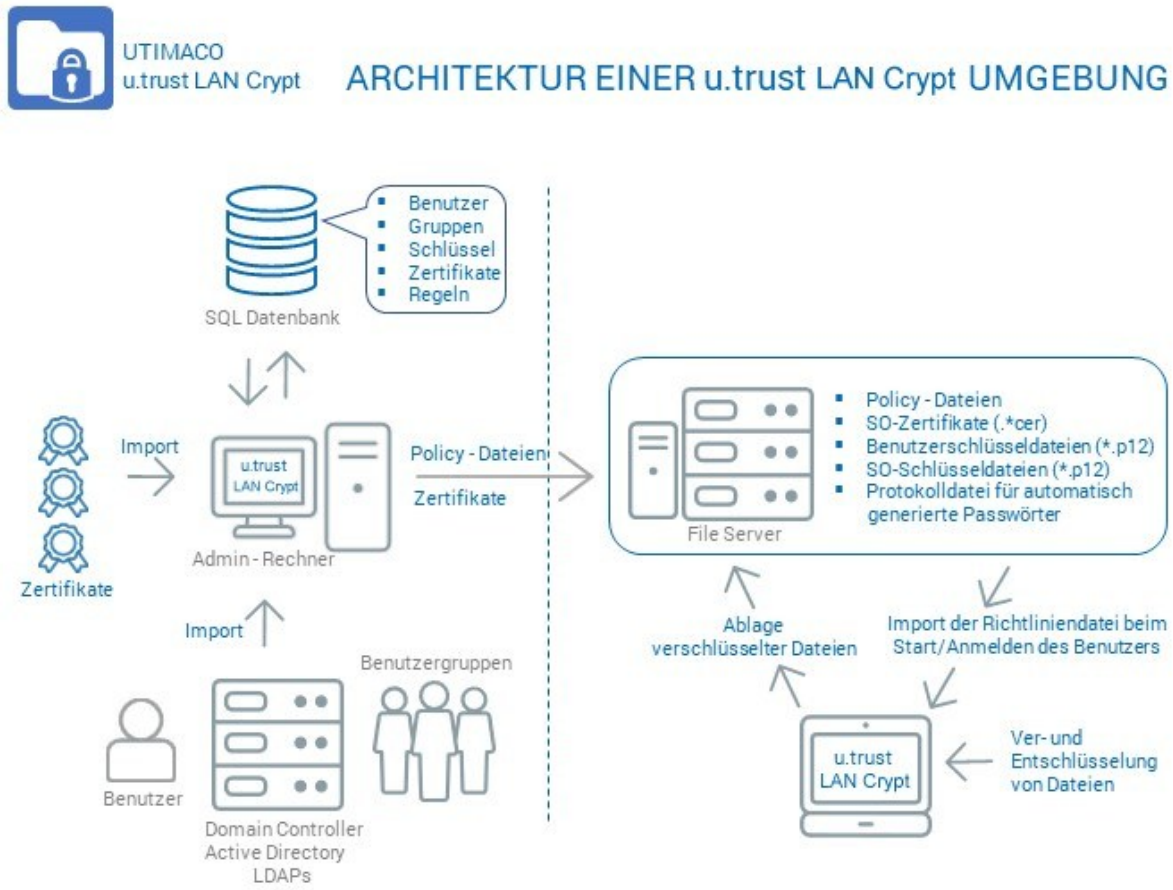
Identifiziert ein DLP-Produkt Daten, die verschlüsselt werden sollen, so kann es die *u.trust LAN Crypt* Client API verwenden, um die Dateien zu verschlüsseln. In der *u.trust LAN Crypt* Administration können Sie unterschiedliche Verschlüsselungs-Tags definieren, die den jeweils zu verwendenden *u.trust LAN Crypt*-Schlüssel vorgeben.

Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden, wie z.B. das Verschlüsselungs-Tag <CONFIDENTIAL>, um dann alle Dateien zu verschlüsseln, die von Ihrem DLP-Produkt als vertraulich kategorisiert sind.

1.4 Architektur

u.trust LAN Crypt besteht aus den beiden Komponenten: Der *u.trust LAN Crypt* Administration und dem *u.trust LAN Crypt* Client. Die Installation beider Komponenten erfolgt typischerweise auf Standard-Arbeitsplatzrechnern mit dem Betriebssystem Windows 11 oder auf einem von *u.trust LAN Crypt* unterstützen Windows Server System. Security Officer nutzen *u.trust LAN Crypt* Administration zur Definition und Verteilung von Verschlüsselungsprofilen und stellt diese dann den Benutzern zur Verfügung.

Die folgende Abbildung veranschaulicht das Zusammenspiel der einzelnen Komponenten und wie sich *u.trust LAN Crypt* in das Unternehmensnetz integriert:



1.4.1 u.trust LAN Crypt Administration

Die Administrationskomponente beinhaltet alle erforderlichen Werkzeuge zur zentralen Verwaltung von *u.trust LAN Crypt* und wird von einem oder mehreren Security Officers genutzt. Typischerweise erfolgt die Installation auf einem oder mehreren Arbeitsplatzrechnern mit Windows 11 als Betriebssystem. Darüber hinaus ist auch die Installation auf einem von *u.trust LAN Crypt* unterstützen Windows Server System (ab Windows Server 2022) möglich, wenn eine zentrale Administration per Windows Terminal Services oder Citrix Metaframe gewünscht ist. Dies ist vor allem in größeren Umgebungen und insbesondere bei verteilten Standorten empfehlenswert. Der Zugriff auf die *u.trust LAN Crypt* Administration erfolgt dann per Remote Desktop (RDP) oder Independent Computing Architecture (ICA) Protokoll.

Genauere Informationen, welche Betriebssystemversionen unterstützt werden, finden Sie in den Release Notes von *u.trust LAN Crypt*.

Da die Sicherheit und Vertraulichkeit der zu schützenden Daten nur dann maximal gewährleistet werden kann, wenn die *u.trust LAN Crypt* Administration und Systemadministration voneinander unabhängig sind, verfügt *u.trust LAN Crypt* über eine separate Benutzer- und Gruppenverwaltung. Zur Arbeitserleichterung können von *u.trust LAN Crypt* verwaltete Benutzer und Gruppen aus einem vorhandenen Active Directory oder einem anderen LDAP-basierenden Verzeichnisdienst importiert werden.

Die *u.trust LAN Crypt* Administration benötigt zur Speicherung von Konfigurationsdaten und zur Verwaltung von *u.trust LAN Crypt* Benutzern und Gruppen eine SQL-Datenbank. Die Datenbank kann lokal auf dem Administrationssystem installiert sein, sofern die Microsoft Express Edition zum Einsatz kommt. Für größere Installationen mit mehreren Security Officern empfiehlt sich der Einsatz eines zentralen Datenbank-Systems in Form eines Microsoft SQL beziehungsweise Oracle Servers.

Security Officer sind mit der Definition der Security Policy einer Organisation betraut. Sie legen die Richtlinien fest und sorgen für deren Umsetzung, Einhaltung und Anpassung. Ein kleines Unternehmen kommt meist mit einem einzigen Security Officer aus. In größeren Organisationen sind häufig mehrere Security Officer gleichzeitig eingesetzt, die meist auf Abteilungs- oder Standortebene arbeiten und entsprechend hierarchisch organisiert sind. Die hieraus resultierenden Hierarchieebenen lassen sich auch mit *u.trust LAN Crypt* abbilden.

An der Spitze einer Organisation stehen dabei ein oder mehrere Master Security Officer, die bei der Erzeugung der *u.trust LAN Crypt* Datenbank anwesend sein müssen. Sie legen die ersten Sicherheitsrichtlinien fest und entscheiden, ob für sicherheitskritische Aktionen ein *Mehr-Augen-Prinzip* zur Anwendung kommen muss. Jeder Security Officer erhält bestimmte Berechtigungen (Permissions) in der Administration, die seine grundsätzlichen Rechte festlegen. Zusätzlich lässt sich sein Aufgabenbereich durch **A**ccess **C**ontrol **L**ists (ACLs) auf wenige Benutzergruppen einschränken.

u.trust LAN Crypt verwaltet die Zugriffsrechte der Anwender mithilfe von **K**ey **E**ncryption **K**eys (KEK). Diese liegen in der SQL-Datenbank, sind verschlüsselt und sind wie alle Datenbankinhalte mit MAC- und Hashwerten vor einer Veränderung geschützt. Die Administration ist so ausgelegt, dass ein Security Officer nur den Namen des Schlüssels, nicht jedoch seinen tatsächlichen Wert kennen muss. So kann er mit Schlüsselobjekten arbeiten und Verschlüsselungsregeln erstellen. Durch die flexible Rechtesteuerung lassen sich verschiedenste Anwendungsszenarien abdecken. Beispielsweise können Abteilungsleiter Schlüssel definieren und Verzeichnisse bzw. Ordner zuweisen. Ein zentraler Security Officer erzeugt in einem weiteren Arbeitsgang dann die Verschlüsselungsprofile. So bleiben die Schlüssel unter zentraler Kontrolle.

u.trust LAN Crypt kennt zwei automatisch generierte Schlüsseltypen: Benutzer- und Gruppenschlüssel. Benutzerschlüssel werden pro Benutzer generiert und können für generische Verschlüsselungsregeln genutzt werden, wie z. B. die Verschlüsselung von *Home Directories* oder von lokalen und temporären Ordnern. Pro Benutzer gibt es genau einen Benutzerschlüssel. Für eine Notfall-Wiederherstellung von per Benutzerschlüssel geschützten

Daten muss der Security Officer diesen Schlüssel explizit einem anderen Benutzer zuweisen. Diese Art von Wiederherstellung benötigt ein besonderes Recht in der Administration und kann an ein *Mehr-Augen-Prinzip* gekoppelt werden, um so möglichen Missbrauch zu verhindern. Auch für Benutzergruppen steht ein ähnliches Konzept in Form von Gruppenschlüsseln zur Verfügung (siehe „Spezifische Schlüssel wieder zuweisen“ auf Seite 135).

Hinweis: Informationen über eine Notfall-Wiederherstellung der *u.trust LAN Crypt*-Administration, wenn beispielsweise das Zertifikat des Master Security Officers beschädigt ist, finden Sie in Kapitel 3.5.10 „Wiederherstellungsschlüssel“ auf Seite 74.

Die Profildateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden. Bevor ein Benutzer auf seiner Arbeitsstation Daten mit *u.trust LAN Crypt* ver- und entschlüsseln kann, muss er in der Lage sein, auf die Verschlüsselungsinformationen, die in seiner Profildatei gespeichert sind, zuzugreifen. Die Profildateien werden daher entweder auf einem Fileserver oder im Netlogon-Share eines Domänencontrollers gespeichert.

Hinweis: Eine Installation von *u.trust LAN Crypt* Komponenten auf File-Servern oder Domänencontrollern ist nicht erforderlich. Zur Erleichterung der Administration der *u.trust LAN Crypt* Benutzergruppen und Clientcomputer kann es aber hilfreich sein, auf einer administrativen Workstation (RSAT) die bei der Admin-Konsole mitgelieferten administrativen Vorlagendateien (*ADMX- und ADML-Dateien*) zu installieren. Diese ermöglichen eine einfache und übersichtliche Administration der wichtigsten Einstellungen für die *u.trust LAN Crypt* Clients.

Profildateien liegen als BZ2-gepackte XML-Dateien vor, sind also eigentlich Klartext, enthalten aber unter anderem die für den jeweiligen Anwender verfügbaren Schlüssel – natürlich in verschlüsselter Form. Um mit ihnen arbeiten zu können, müssen sie mithilfe des **P**rofile **E**ncryption **K**eys (PEK) entschlüsselt werden.

Dazu vergleicht der Profil-Lader des *u.trust LAN Crypt* Clients die in der Profildatei gelisteten Zertifikate mit den Zertifikaten im Zertifikatsspeicher des angemeldeten Benutzers. Wenn der Profil-Lader eine Übereinstimmung findet, überträgt er der *Crypto API* die Aufgabe, den dazu passenden PEK zu extrahieren. Diese wiederum aktiviert den **C**ryptographic **S**ervice **P**rovider (CSP) oder **K**ey **S**torage **P**rovider (KSP) mit dem zugehörigen privaten Schlüssel. Abhängig vom Typ des Providers wird der Anwender unter Umständen aufgefordert, eine PIN oder ein Passwort einzugeben. Danach wird das Profil entschlüsselt und zum Filter-Treiber geschickt. *u.trust LAN Crypt* unterstützt zudem auch die Verwendung von Zertifikaten auf Smartcards, USB-Sicherheitstoken oder geeigneten Hardware-Boards.

Hinweis: Die Verwendung von Smartcards oder Sicherheitstoken zur Speicherung von Zertifikaten ist keine Voraussetzung für den Einsatz von *u.trust LAN Crypt*.

Die Pfade zu den Profildateien (vom Standpunkt des Benutzers aus) und andere *u.trust LAN Crypt* Einstellungen werden durch Mechanismen im Betriebssystem erkannt.

Eine *u.trust LAN Crypt* Berechtigungsgruppe wird durch Benutzer mit demselben Verschlüsselungsprofil gebildet. In der Administration werden Profildateien für jeden einzelnen Benutzer

erzeugt. Alle *u.trust LAN Crypt* Benutzer, die in ihrer Profildatei dieselben Regeln gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Die Benutzer müssen sich dazu weder um die Verschlüsselung noch um den Schlüsselaustausch kümmern. Sie müssen nur in der Lage sein, auf ihre Profildateien zuzugreifen, und ihre Dateien werden transparent ver- bzw. entschlüsselt, sobald sie geöffnet bzw. geschlossen werden.

1.4.2 u.trust LAN Crypt Client

Die *u.trust LAN Crypt* Client-Anwendung wird auf den Windows-Systemen (PC, Workstation, Notebook, Terminal Server) installiert, auf denen eine Verschlüsselung stattfinden soll. Die Client-Komponente bietet neben dem zur Ver- und Entschlüsselung obligatorischen Filtertreiber (Minifilter) noch folgende optionale Komponenten:

- Explorer-Erweiterungen zur initialen und expliziten Verschlüsselung.
- Benutzerprogramm zum Laden und Löschen von Verschlüsselungsregeln, sowie Aktivieren und Deaktivieren der Verschlüsselung.
- Benutzerprogramm zum Anzeigen aller am Client wirksamen Einstellungen und Regeln. Dies ist vor allem für Support-Fälle wichtig.
- Benutzerprogramm zur Initialverschlüsselung.
- Token Support zur Verwendung von Token-basierten Zertifikaten für den Zugriff auf die gespeicherten Verschlüsselungsinformationen.
- Netzwerkfiltertreiber, der die Performance bei Netzwerkzugriffen verbessern hilft.
- Client-API, um bestimmten Applikationen (z. B. DLP-Produkte) den Zugriff auf die *u.trust LAN Crypt* Dateiverschlüsselungsfunktion zu ermöglichen.

Nach dem Start des *u.trust LAN Crypt* Clients greift dieser über Mechanismen des Betriebssystems (Registry-Einstellungen, Gruppenrichtlinien) auf die Ordner mit seinem PCKS#12-Container (*.P12-Datei) und seiner Profildatei zu. Beim ersten Zugriff auf den PKCS#12-Container muss vom Benutzer ein Passwort eingegeben werden, das ihm ein Security Officer auf abgesichertem Weg mitteilt (siehe Abschnitt 3.5.6 „*Passwortprotokolldatei*“ auf Seite 44). Danach wird das Benutzer-Zertifikat im lokalen Zertifikatspeicher des Betriebssystems abgelegt, also mit dem geladenen Windows-Profil verknüpft. Das Zertifikat erlaubt über den „**P**rofile **E**ncryption **K**ey – PEK” den Zugriff auf die verschlüsselten Teile der Profildatei. Ist das Zertifikat auf einem von der Clientkomponente unterstützten Hardware-basierten Token abgelegt, so ist nach dem Entsperren des Tokens keine weitere Benutzerinteraktion zur Ver- und Entschlüsselung erforderlich.

Anschließend lädt der *u.trust LAN Crypt* Client die Profildatei mit ihren Einstellungen und Schlüsseln.

2 Erste Schritte

2.1 Zertifikate

u.trust LAN Crypt verwendet Zertifikate und Public / Private Key Schlüsselpaare zur Sicherung der in Profildateien gespeicherten Verschlüsselungsinformationen. Nur der Besitzer des Zertifikats hat Zugriff auf den zum Zertifikat gehörenden privaten Schlüssel und kann ihn daher zum Zugriff auf die Verschlüsselungsinformationen verwenden.

Hinweis: Bitte verwenden Sie grundsätzlich keine Zertifikate, deren Gültigkeit mehrere hundert oder gar mehr als tausend Jahre betragen!

Im Sinne der Informationssicherheit sollte die Gültigkeitsdauer von Zertifikaten einen Zeitraum von 5 Jahren nach Möglichkeit nicht überschreiten. Für CA-Zertifikate (**C**ertificate **A**uthority) empfiehlt Utimaco dagegen eine maximale Gültigkeitsdauer von 20 Jahren.

Welche Zertifikate verwendet werden können und woher sie kommen:

- Ein Unternehmen verfügt über eine eigene **P**ublic **K**ey **I**nfrastructure (PKI) oder nutzt ein Trust Center, um Zertifikate für die Benutzer zu erzeugen. Vorhandene Zertifikate können in diesem Fall verwendet werden.
- Die Administration von *u.trust LAN Crypt* kann optional selbst-signierte Zertifikate erzeugen. Diese Zertifikate können ausschließlich von *u.trust LAN Crypt* verwendet werden! Die Zertifikate sind zudem mit einer kritischen Erweiterung versehen, um anderen Applikationen anzuzeigen, dass sie nicht verwendet werden dürfen. Es handelt sich um einfache Zertifikate (vergleichbar mit Klasse-1-Zertifikaten), die aber dem X.509-Standard entsprechen.

In *u.trust LAN Crypt* können Sie festlegen, ob zu einem neu erzeugten Zertifikat eine kritische Erweiterung (OID) hinzugefügt werden soll oder nicht.

Hinweis: Einzelne Applikationen ignorieren unter Umständen diese kritische Erweiterung der *u.trust LAN Crypt* Zertifikate. Dies führt dann zu Problemen mit diesen selbst-signierten Zertifikaten. Deaktivieren Sie in diesem Fall explizit alle Nutzungszwecke für die *u.trust LAN Crypt* Zertifikate über das Zertifikate-Snap-In der Microsoft Management Console (MMC), um die Verwendung des Zertifikats in anderen Applikationen zu verhindern.

Hinweis: Wenn Sie einstellen, dass neuen Zertifikaten eine kritische Erweiterung hinzugefügt werden soll, wird bei einem solchen Zertifikat, wenn Sie sich dessen Zertifikatsinformationen anzeigen lassen, der Status: „*Ein Zertifikat enthält eine unbekannte Erweiterung, die als kritisch gekennzeichnet ist*“ angezeigt. Sie können diese Information jedoch getrost ignorieren, da *u.trust LAN Crypt* die *OID* (Objekt-Identifikation) der eigenen Zertifikate kennt und diese daher als gültig anerkennt.

Die Zertifikate werden den Benutzern in der *u.trust LAN Crypt* Administration zugewiesen.

Im Folgenden erhalten Sie einige wichtige Informationen zur Verwendung von Zertifikaten:

- *u.trust LAN Crypt* verwendet das Microsoft Crypto API ausschließlich für die Zertifikatsfunktionalität.
- *u.trust LAN Crypt* unterstützt ab Version 13.0.1 **K**ey **S**torage **P**rovider (KSP).
- *u.trust LAN Crypt* unterstützt alle **C**ryptographic **S**ervice **P**rovider (CSP), die bestimmte Sicherheitsstandards erfüllen (z. B. RSA-Schlüssellänge mit mindestens 2048 Bit).

  Hinweis: Der Microsoft-Standard CSP (Microsoft Base CSP) kann für selbst-signierte Zertifikate, die von *u.trust LAN Crypt* erzeugt wurden, nicht verwendet werden.

  Hinweis: Bitte beachten Sie auch, dass **C**ryptographic **S**ervice **P**rovider (CSP) für Schlüsseloperationen von *u.trust LAN Crypt* nur noch in Verbindung mit Shims unterstützt werden, die diesen als **K**ey **S**torage **P**rovider (KSP) ansprechbar machen.

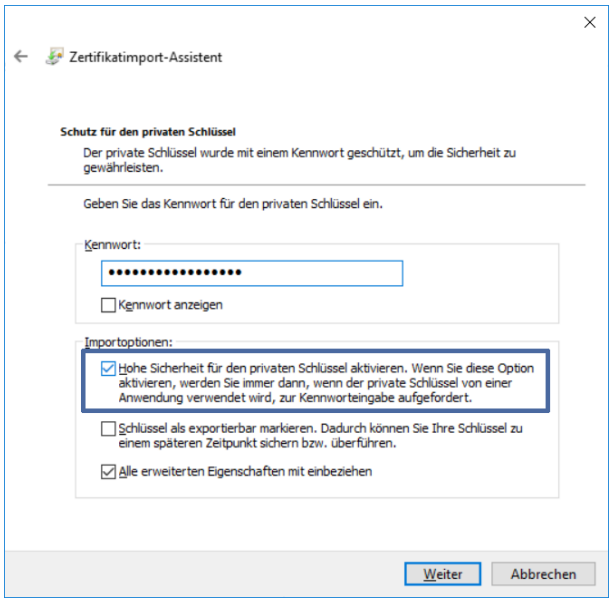
  Hinweis: Der Signatur-Algorithmus SHA-1 wird nicht mehr unterstützt, da dieser als nicht mehr sicher gilt.

Sollten Sie Fragen bezüglich der Kompatibilität anderer CSPs oder KSPs haben, kontaktieren Sie bitte den Utimaco-Support (siehe “*Technischer Support*„ auf Seite 205).

Hinweis: ECC-Zertifikate (basierend auf Elliptische-Kurven-Kryptografie) werden von *u.trust LAN Crypt* derzeit nicht unterstützt.

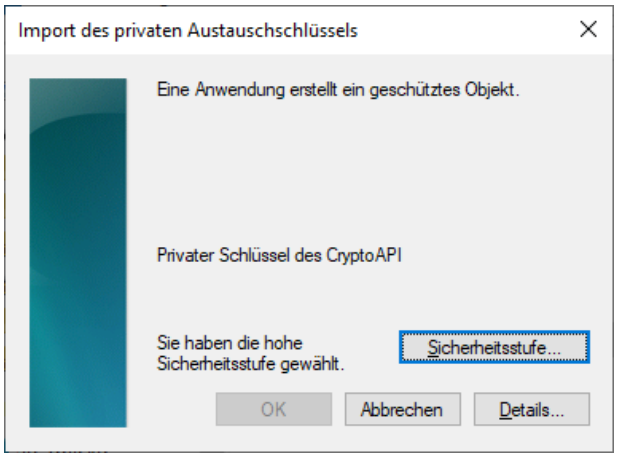
2.1.1 Sicherheitsniveau

Da *u.trust LAN Crypt* das höchstmögliche Sicherheitsniveau anstrebt, empfehlen wir beim Import eines Zertifikats über den *Zertifikatsimport-Assistent* die Option „*Hohe Sicherheit für den privaten Schlüssel*“ zu aktivieren.



Klicken Sie in den beiden darauffolgenden Dialogen jeweils auf **Weiter** und danach auf **Fertig stellen**. Nachdem Sie im *Zertifikatimport-Assistent* auf **Fertig stellen** geklickt haben, wird der Dialog *Import des privaten Austauschschlüssels* angezeigt.

Durch Klicken auf die Schaltfläche **Sicherheitsstufe** können Sie noch einmal die Sicherheitsstufe bestimmen:



- **Hoch**

  Wenn Sie *Hoch* wählen, müssen Sie die Verwendung des privaten Schlüssels durch die Eingabe eines Kennworts bestätigen. Im folgenden Dialog kann dann ein neues Kennwort angegeben werden.

- **Mittel**

  Wenn Sie *Mittel* wählen, wird eine Meldung angezeigt, in der Sie die Verwendung des privaten Schlüssels durch Klicken auf **OK** bestätigen müssen.

Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie je nach Einstellung der Sicherheitsstufe dann entweder zur **Eingabe des Kennworts** (hohe Sicherheitsstufe) oder zum Klicken auf **OK** (mittlere Sicherheitsstufe) aufgefordert.

Höchstes Sicherheitsniveau bei automatisch importierten Schlüsselaustausch-Dateien (.p12, .pfx)

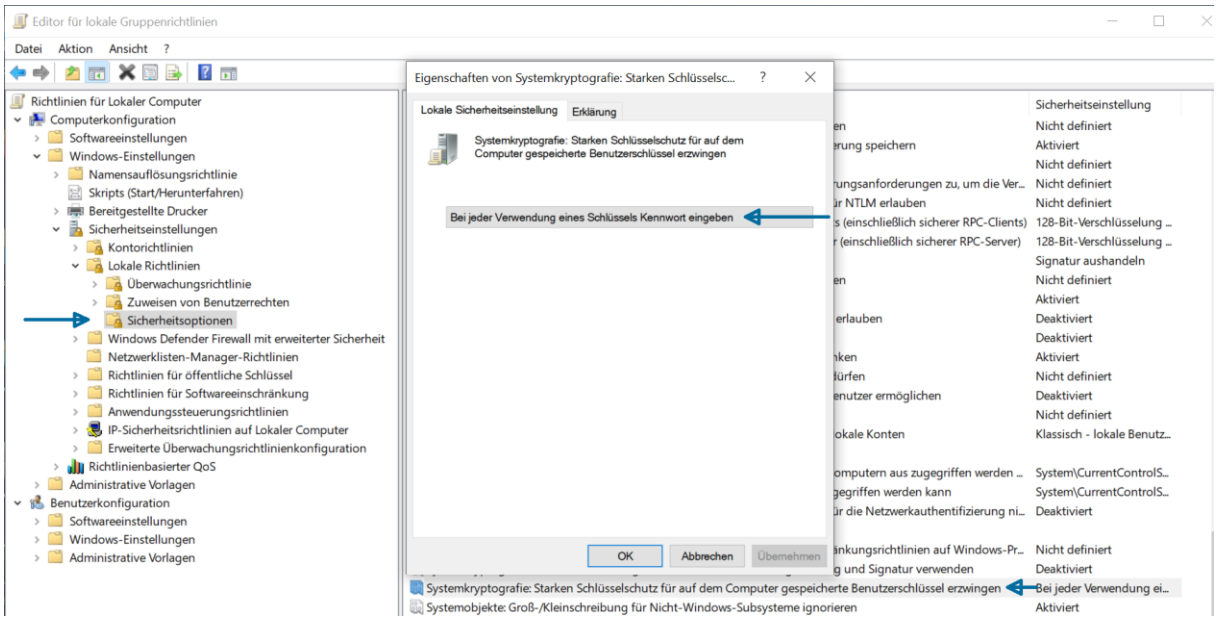
u.trust LAN Crypt bietet die Möglichkeit, Zertifikate automatisch zu importieren. Um bei den zu diesen Zertifikaten gehörenden privaten Schlüsseln die mittlere bzw. hohe Sicherheitsstufe anzuwenden, stellen Sie die Option **Hohe Sicherheit für den privaten Schlüssel** in der *u.trust LAN Crypt* Konfiguration auf **Ja** ein (siehe Abschnitt 4.1.18 „*Hohe Sicherheit für den privaten Schlüssel*“ auf Seite 186.

Auf diese Weise kann im Sinne eines unternehmensweiten Sicherheitskonzepts die verpflichtende Verwendung von Zertifikaten mit einer hohen Sicherheitsstufe durchgesetzt werden.

Wird diese Einstellung nicht vorgenommen, wird für die so importierten Benutzerzertifikate automatisch die niedrige Sicherheitsstufe angewendet.

Hinweis: Für einen *u.trust LAN Crypt* Benutzer bedeutet die Verwendung der höchsten Sicherheitsstufe, dass er das Kennwort für den privaten Schlüssel einmal bei der Anmeldung und immer, wenn „manuell“ eine Verschlüsselungsregel geladen wird, eingeben muss.

Aktivieren Sie auch die lokale Windows Gruppenrichtlinie „*Systemkryptografie: Starken Schlüsselschutz für auf dem Computer gespeicherte Benutzerschlüssel erzwingen*“ und wählen Sie die Option „*Bei jeder Verwendung eines Schlüssels Kennwort eingeben*“. Damit stellen Sie die Sicherheitsstufe immer auf „hoch“ ein.



Smartcard:

Werden auf Smartcard gespeicherte Zertifikate verwendet, so muss das Passwort nur einmal eingegeben werden. Solange sich die Smartcard im Kartenleser befindet, ist eine Eingabe für das Passwort nicht erneut erforderlich.

Achtung: Wir empfehlen vor dem ersten Start der *u.trust LAN Crypt* Administration die Aktivierung der *Hohen Sicherheit für den privaten Schlüssel*. Anderenfalls wird das Zertifikat des initialen Master Security Officers, wenn dieses von *u.trust LAN Crypt* erzeugt wird und nicht z. B. von einer Smartcard importiert wird, ohne hohe Sicherheit verwendet.

Achtung: Die PINs werden von Windows standardmäßig 24 Stunden zwischengespeichert. Bei der Verwendung von Software-Zertifikaten kann dies bei der Anmeldung an die Administration und beim Ausführen einer zusätzlichen Autorisierung zu Sicherheitsproblemen führen. Es wird daher dringend empfohlen, diese Funktionalität zu deaktivieren.

Setzen Sie dafür die folgenden Werte:

```
"CachePrivateKeys"=dword:00000001
"PrivateKeyLifetimeSeconds"=dword:00000005
"PrivKeyCacheMaxItems"=dword:00000000
"PrivKeyCachePurgeIntervalSeconds"=dword:00000000
```

unter dem Schlüssel:

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography
```

sowie den Wert:

```
"AllowCachePW"=dword:00000000
```

unter dem Schlüssel:

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography\
Protect
```

In diesem Fall werden PINs für private Schlüssel nicht mehr zwischengespeichert.

Hinweis: Wenn Sie „`CachePrivateKeys`“ den Wert „0“ und „`PrivateKeyLifetimeSeconds`“ einen Wert zuweisen, der kleiner als „5“ ist, kann das dazu führen, dass ein (Master) Security Officer die PIN beim Import eines Zertifikats (**.p12-Datei*) in den Windows Zertifikatsspeicher doppelt eingeben muss.

Vorbedingungen zur Verwendung von Zertifikaten mit u.trust LAN Crypt

- Das Zertifikat muss einen öffentlichen Schlüssel enthalten.
- Um Zugriff auf die Verschlüsselungsvorschriften zu erhalten, muss der private Schlüssel des zugewiesenen Zertifikats verfügbar sein.
- Nur Zertifikate, die unter *Benutzerkonfiguration* in den Zertifikatsspeichern *Eigene Zertifikate*, *Andere Personen* und *Active Directory-Benutzerobjekt* sowie unter *Richtlinien für Lokaler Computer* im Zertifikatsspeicher *Eigene Zertifikate* gespeichert sind, werden von *u.trust LAN Crypt* aufgelistet. Zertifikate, die an anderen Orten gespeichert sind, werden von *u.trust LAN Crypt* nicht berücksichtigt.

  Zertifikate können mit dem Zertifikats-Snap-In für die Management Konsole importiert und verwaltet werden.
- Zum „Verbinden“ eines Zertifikats mit den *u.trust LAN Crypt* Verschlüsselungs-informationen wird nur der öffentliche Schlüssel verwendet. Der private Schlüssel muss nicht bekannt sein. Der private Schlüssel bleibt immer im Eigentum des Besitzers und nur er ist dann imstande auf die Verschlüsselungsinformationen zuzugreifen.

Es ist empfehlenswert, die Zertifikate zur Verfügung zu haben, bevor mit der Installation von *u.trust LAN Crypt* begonnen wird. Auf diese Weise werden sie sofort nach der Installation in der Microsoft Management Konsole unter *Zertifikate* angezeigt und können verwendet werden.

Hinweis: Die Verwaltung von Zertifikaten ist keine Aufgabe von *u.trust LAN Crypt*. Die Zertifikatsverwaltung kann mittels einer firmeneigenen PKI (**P**ublic-**K**ey-**I**nfrastruktur) oder mittels eines Trust Centers durchgeführt werden.

2.1.2 Zertifikatsprüfung

u.trust LAN Crypt erlaubt es, eine erweiterte Zertifikatsprüfung durchzuführen. Dies bedeutet, dass Zertifikate nur akzeptiert werden, wenn Sie vollständig überprüft werden können (Auswertung einer **C**ertificate **R**evocation **L**ist).

In der *u.trust LAN Crypt* Administration wird diese Zertifikatsprüfung für folgende Zertifikate angewendet:

- Für die Zertifikate, die beim Anlegen des initialen Master Security Officers angeboten werden. Es werden nur Zertifikate angeboten, die vollständig überprüft werden konnten.
- Für die Zertifikate, die nach der Verwendung des Wiederherstellungsschlüssels angeboten werden, um einem Security Officer ein neues Zertifikat zuzuweisen. Es werden nur Zertifikate angeboten, die vollständig überprüft werden konnten.
- Für die Zertifikate der Security Officer, die sich an die *u.trust LAN Crypt* Datenbank anmelden. Kann das Zertifikat nicht vollständig überprüft werden, ist keine Anmeldung möglich.
- Für Zertifikate von Security Officers, die im Rahmen der zusätzlichen Autorisierung verwendet werden.

Die erweiterte Zertifikatsprüfung erfordert folgende Voraussetzungen:

- In dem verwendeten Zertifikat ist eine CRL eingetragen.

  Manche PKIs erlauben es, ein Zertifikat in eine CRL einzutragen. Ist ein solcher Eintrag vorhanden, wird diese Liste ausgewertet. Hierzu muss bei Bedarf eine CRL des Ausstellers über das Netzwerk geladen werden. Kann das Zertifikat nicht überprüft werden, wird es nicht zur Auswahl angeboten bzw. nicht zur Anmeldung akzeptiert.

- Eine CRL wurde in den lokalen Zertifikatsspeicher geladen.

Hinweis: Bitte beachten Sie, dass zur Auswertung einer CRL eine Netzwerkverbindung notwendig sein kann. Kann die Verbindung nicht hergestellt werden, so wird der Zugriff verweigert, auch wenn das Zertifikat eigentlich gültig wäre.

2.1.3 Smartcard Leser

Da die Benutzung von Zertifikaten durch die Verwendung von **C**ryptographic **S**ervice **P**rovidern (CSPs) und **K**ey **S**torage **P**rovidern (KSPs) abgewickelt wird, werden Smartcard-Leser automatisch unterstützt, wenn ein Smartcard-KSP verwendet wird. Der Zugriff auf die gespeicherten Verschlüsselungsinformationen kann so über ein auf Smartcard gespeichertes Zertifikat erfolgen.

Hinweis: Wenn Sie Zertifikate auf Smartcards verwenden wollen, stellen Sie bitte sicher, dass der Smartcard Leser, die dazugehörige Middleware und ein entsprechender Service- oder Storage-Provider (CSP oder KSP) korrekt installiert sowie funktionsbereit sind!

Hinweis: Bitte beachten Sie außerdem, dass **C**ryptographic **S**ervice **P**rovider (CSP) für Schlüsseloperationen von *u.trust LAN Crypt* nur noch in Verbindung mit Shims unterstützt werden, die diesen als **K**ey **S**torage **P**rovider (KSP) ansprechbar machen.

2.2 Installation

Typischerweise erfolgt die Installation auf einem oder mehreren Arbeitsplatzrechnern mit Windows 11 als Betriebssystem oder auf einem von *u.trust LAN Crypt* unterstützen Windows Server System.

Hinweis: Die Installation von *u.trust LAN Crypt* ist nur möglich, wenn Sie mit Administratorrechten an dem Betriebssystem angemeldet sind.

1. Wählen Sie das Installationsverzeichnis Ihres extrahierten Installationspakets und doppelklicken Sie auf die Datei *LCAdmin.msi*.

   Ein Installations-Assistent führt Sie durch die sehr einfache Installation von *u.trust LAN Crypt*. Klicken Sie auf **Weiter**.

2. Der Dialog *Lizenzbedingungen* wird angezeigt.

   Bitte aktivieren Sie die Option **Ich stimme den Bedingungen der Lizenzvereinbarung zu**. Wenn Sie dies nicht tun, ist eine Installation von *u.trust LAN Crypt* nicht möglich! Klicken Sie auf **Weiter**.

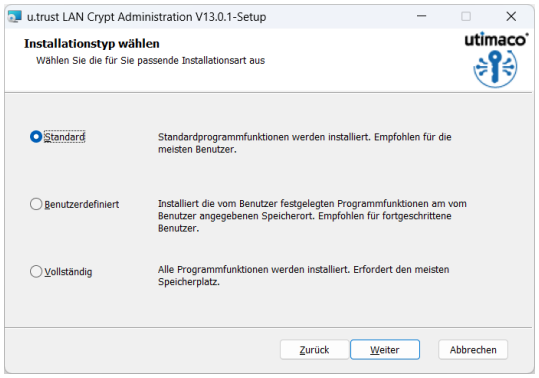
3. Der Dialog *Zielordner* wird angezeigt.

   Wählen Sie aus, unter welchem Pfad *u.trust LAN Crypt* Administration installiert werden soll. Wenn Sie diese Einstellung nicht ändern, erfolgt die Installation unter:

   ```
   <Systemlaufwerk>:\Programme (x86)\utimaco\u.trust LAN Crypt\Administration\
   ```

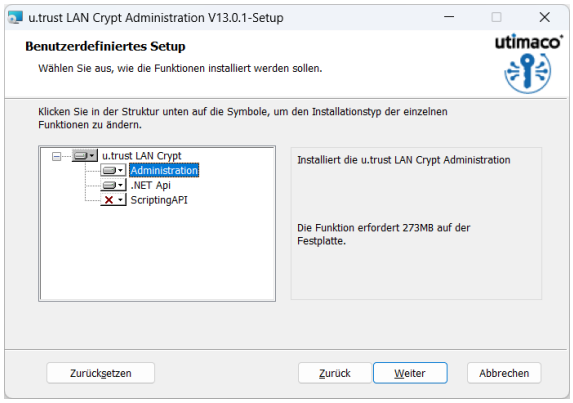
   Klicken Sie auf **Weiter**.

4. Der Dialog *Installationstyp wählen* wird angezeigt.

   In diesem Dialog können Sie je nach gewähltem Installationstyp auswählen, welche Komponenten von *u.trust LAN Crypt* Administration installiert werden sollen. Wählen Sie den von Ihnen gewünschten Installationstyp und klicken Sie auf **Weiter**.

Wenn Sie **Benutzerdefiniert** gewählt haben, können Sie die Komponenten selbst auswählen, die installiert werden sollen:



- **Administration**

  Installiert die *u.trust LAN Crypt* Administration.

- **ScriptingAPI**

  Installiert das *u.trust LAN Crypt ScriptingAPI* für die Skript-gesteuerte Administration von *u.trust LAN Crypt*.

  Hinweis: Anders als im Vergleich zu früheren *LAN Crypt* Versionen ist bei der benutzerdefinierten Installation standardmäßig *.NET-API* statt *ScriptingAPI* aktiviert.

- **.NET API**

  Installiert das *u.trust LAN Crypt .NET API* für die Skript-gesteuerte Administration von *u.trust LAN Crypt* sowie einige Beispielskripte.

  Hinweis: *u.trust LAN Crypt .NET API* können Sie ab Version 13.0.0 auch ohne weitere Programmfunktionen bzw. Komponenten installieren.

  Hinweis: Wenn Sie bei der Nutzung der *.NET API* eine Fehlermeldung erhalten, prüfen Sie bitte, ob auch der u. a. Paketverweis (PackageReference) in Ihrem Projekt enthalten ist:

  ```
  <PackageReference Include="Microsoft.Win32.Registry" Version="5.0.0" />
  ```

  Hinweis: Wenn die *u.trust LAN Crypt* Administration nicht über das im Installationsordner enthaltende MSI-Paket installiert wird, sondern über einen eigenen Installer, **muss** auch der für das *.NET API* erforderliche Registry-Key gesetzt werden. Für die 32 Bit *.NET API*:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\conpal\LAN Crypt\Admin\Setup]
  "InstallDir"="C:\\Program Files (x86)\\utimaco\\u.trust LAN Crypt\\Administration\\"
  ```

  Für die 64 Bit *.NET API*:

  ```
  [HKEY_LOCAL_MACHINE\SOFTWARE\conpal\LAN Crypt\Admin\Setup]
  "InstallDir"="C:\\Program Files\\Utimaco\\u.trust LAN Crypt\\Administration\\"
  ```

  Sie müssen unter „`InstallDir`“ den Pfad eintragen, unter dem sich die DLLs der *u.trust LAN Crypt* Administration befinden. Standardmäßig ist das jeweils der unter „`InstallDir`“ eingetragene Pfad.

Wenn Sie *u.trust LAN Crypt* **nicht** im Standardpfad installiert haben, beachten Sie den folgenden **Hinweis:** Möchten Sie die mitgelieferten Beispielskripte nutzen, müssen in den jeweiligen Skripten die Pfadangaben zu den API-DLLs analog zum geänderten Installationspfad angepasst werden.

Hinweis: Das *.NET SDK* ist nur für die Nutzung von cs-Skripten / Projekten erforderlich, nicht jedoch für Powershell-Skripte.

Das Beispielprogramm *StartFirstHere* ist standardmäßig für *.NET Core 8.0* eingerichtet.

Beachten Sie: Wenn Sie die **64 Bit Version der *.NET API*** verwenden wollen, muss auch eine **64 Bit ODBC Verbindung zur *LAN Crypt*** **Datenbank** eingerichtet werden bzw. eine solche bestehen. Alle dazugehörigen API-Bibliotheksdateien (DLLs) müssen sich im gleichen Verzeichnis wie die Anwendung befinden und über die Umgebungsvariable „`PATH`“ gefunden werden können.

Dies betrifft die folgenden Dateien:

- *LCAdminApiNetX64.dll*
- *LCNetApiX64.dll*
- *SGLCScriptApiV4.dll*
- *sglcapi.dll*
- *LCDA.dll*

5. Wählen Sie aus, welche Komponenten installiert werden sollen und klicken Sie danach auf **Weiter**.

Hinweis: Wenn Sie die Option **Standard** gewählt haben, wird nur die *Administration*, bei Auswahl von **Vollständig** werden auch das *u.trust LAN Crypt ScriptingAPI* und *.NET API* installiert.

6. Nachdem Sie Ihre Angaben noch einmal geprüft haben, klicken Sie auf **Installieren** im Installationsvorbereitungsdialog. Die Installation wird gestartet.

7. Bei erfolgreicher Installation erscheint ein Dialogfenster. Klicken Sie dort auf **Fertigstellen**, um die Installation abzuschließen.

Hinweis: Um die Einstellungen vollständig zu übernehmen, müssen Sie das System neu starten! Damit werden auch alle Treiber geladen.

2.3 Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von *u.trust LAN Crypt* auf einer großen Anzahl von Rechnern.

Der *u.trust LAN Crypt*-Installationsordner Install enthält die Datei lcadmin.msi, die für die Installation ohne Benutzerinteraktion erforderlich ist.

2.3.1 Installierbare Komponenten

Die folgende Liste zeigt alle Komponenten, die Sie installieren können und die Art und Weise, wie sie bei der Installation ohne Benutzerinteraktion angegeben werden müssen.

Die Schlüsselwörter geben an, wie die einzelnen Komponenten über `AddLocal=` angegeben werden müssen, wenn eine Installation ohne Benutzerinteraktion ausgeführt wird.

Bei den Bezeichnungen der einzelnen Schlüsselwörter für die Komponenten wird zwischen Groß- und Kleinschreibung unterschieden!

`AddLocal=`**`Administration`**

Installiert nur die *u.trust LAN Crypt* Administration.

`AddLocal=`**`Administration,ScriptApi`**

Neben der *u.trust LAN Crypt* Administration wird auch die ScriptingAPI installiert.

`AddLocal=`**`Aministration,AdminApiDotnet`**

Neben der *u.trust LAN Crypt* Administration wird auch die AdminApi (.NET) installiert.

Beispiel:

```
msiexec /i lcadmin.msi /qn AddLocal=Administration
```

Im o. g. Beispiel wird ohne Benutzerinteraktion nur die *u.trust LAN Crypt* Administration installiert.

Hinweis: Wenn Sie keine Komponente angeben, wird eine vollständige Installation der *u.trust LAN Crypt* Administration durchgeführt.

Hinweis: Mit der Installation der *.NET API* (*AdminApiDotnet*) werden auch Beispielskripte installiert. Standardmäßig erfolgt die Installation für 64 Bit unter:

```
<Laufwerk>:\Programme\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Laufwerk>:\Programme\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

und für 32 Bit unter:

```
<Laufwerk>:\Programme (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API PowerShell Samples\
<Laufwerk>:\Programme (x86)\Utimaco\u.trust LAN Crypt\Administration\Admin API Dotnet Samples\
```

Hinweis: Beachten Sie auch die weiteren Hinweise für das *.NET API* ab Seite 26.

2.3.2 Kommandozeilensyntax

Zum Ausführen einer Installation ohne Benutzerinteraktion muss `msiexec` mit bestimmten Parametern aufgerufen werden.

Unbedingt erforderliche Parameter:

`/I`

Gibt das Installations-Package an, das zu installieren ist.

`/QN`

Installation ohne Benutzerinteraktion.

Name der .msi-Datei: *lcadmin.msi*

Syntax: `msiexec /i <Pfad>\lcadmin.msi /qn`

Optionale Parameter:

`/L*xv <Pfad + Dateiname>`

Protokolliert den gesamten Installationsvorgang in dem unter <Pfad + Dateiname> angegebenen Speicherort.

Beispiel:

```
msiexec /i C:\Install\lcadmin.msi /qn /L*xv c:\Log\log.txt
```

Die Installation von *u.trust LAN Crypt* wird ausgeführt. Das Programm wird im Standardordner (`<Systemlaufwerk>:\Programme (x86)\utimaco\u.trust LAN Crypt Windows\Administration`) installiert.

Die .msi-Datei befindet sich im Ordner *Install* des Installationslaufwerks von *u.trust LAN Crypt*.

Hinweis: Die Speicherung der Administrationsdaten von *u.trust LAN Crypt* erfolgt in einer SQL-Datenbank. Nachdem Sie *u.trust LAN Crypt* Administration erfolgreich installiert haben, müssen Sie diese ggf. noch einrichten (siehe Abschnitt 3.1 „*Notwendige Schritte*“ auf Seite 37).

2.4 Upgrade

Für ein Upgrade der *LAN Crypt* Version 4.2.0 auf diese Version der *u.trust LAN Crypt* Administration ist zunächst ein Zwischen-Upgrade auf die u.trust *LAN Crypt* Version 11.0.x erforderlich (das beinhaltet die Installation selbst und das Upgrade der *LAN Crypt* Datenbank). Danach installieren Sie die aktuelle *u.trust LAN Crypt* Administration Version 13.0.1 und aktualisieren Sie anschließend die bestehende *LAN Crypt* Datenbank mithilfe des Kommandozeilentools `CreateTables.exe`. Die jeweils hierzu erforderlichen Schritte finden Sie auf den folgenden Seiten näher beschrieben.

Hinweis: Wenn Sie eine *LAN Crypt* Version verwenden, die älter als Version 3.90 ist, müssen Sie diese zunächst auf die Version 3.97 und danach auf Version 4.2.0 upgraden.

Hinweis: Die erste Anmeldung nach einem Upgrade muss immer von einem Master Security Officer durchgeführt werden.

2.4.1 Upgrade auf die neue Version

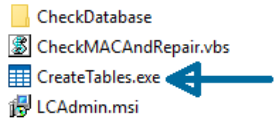
Installieren Sie die neue Version zunächst wie im Abschnitt 2.2 „*Installation*“ auf Seite 25 beschrieben.

Hinweis: Stellen Sie sicher, dass alle Instanzen der *LAN Crypt* Administration geschlossen sind, bevor Sie die neue Version installieren. Es dürfen während des Upgrades keine weiteren (Master) Security Officer mit der *LAN Crypt* Datenbank verbunden sein, da dies zu Inkonsistenzen in der Datenbank führen kann!

Hinweis: Beachten Sie, dass **nach dem Upgrade der *LAN Crypt* Administration auf Version 13.0.0 oder höher kein Mischbetrieb mit früheren LAN Crypt Versionen mehr möglich ist!** Alle zusätzlichen *LAN Crypt*-Administrationen müssen zeitgleich aktualisiert werden. **Ein Zugriff auf eine frühere *LAN Crypt* Datenbank ist ab Version 13.0.0 nicht möglich.** Eine frühere Datenbank muss zuvor zwingend auf die neue Version migriert werden, bevor ein Zugriff mit der *LAN Crypt* Administration auf diese wieder möglich ist.

2.4.2 Upgraden der bestehenden u.trust LAN Crypt Datenbankstruktur

Mit dem Kommandozeilen-Tool `CreateTables.exe` können Sie die Struktur der Tabellen in Ihrer *u.trust LAN Crypt* Datenbank aktualisieren. Sie finden das Tool im *\Install-Ordner* Ihres *u.trust LAN Crypt* Installationspakets.



Hinweis: Erstellen Sie vor dem Upgrade eine Sicherung Ihrer *LAN Crypt* Datenbank.

Für das Upgrade einer bestehenden *u.trust LAN Crypt* Datenbankstruktur empfiehlt Utimaco, dies durch die **IT-Administration** oder einen **Datenbank-Administrator** durchführen zu lassen, da hierfür weitergehende Datenbankrechte (db-Rolle: `db_ddladmin`) erforderlich sind. Beim Datenbank-Upgrade durch `CreateTables.exe` müssen in der *u.trust LAN Crypt* Datenbank neue Tabellen angelegt und u. a. auch DDL-Trigger entfernt werden können.

Hinweis: Die Anmeldung an der Datenbank muss mit Berechtigungen erfolgen, die das Erzeugen und Ändern des Datenbankschemas ermöglichen. Für die Nutzung der *u.trust LAN Crypt* Admin-Konsole sind für Security Officer die Datenbank-Rollen "`db_datareader`" und "`db_datawriter`" jedoch ausreichend.

Kommandozeilensyntax:

```
CreateTables <ODBCName[.Besitzer-Name]> <SQL-Dialekt> <Aktion>
```

CreateTables.exe bietet die folgenden Parameter zur Tabellenerstellung in anderen Konfigurationen:

ODBCName:

Der Name, den Sie für die ODBC-Datenquelle verwendet haben.

Datenbank Besitzer-Name

Damit die Datenbank korrekt angesprochen werden kann, muss für Oracle-Datenbanken auch der Datenbankbesitzer in GROSSBUCHSTABEN mit angegeben werden. Falls das Standard-Schema Ihres Microsoft SQL-Servers nicht *.dbo* entspricht, müssen Sie für Microsoft SQL-Datenbanken den Datenbankbesitzer *.dbo* mit angeben.

SQL-Dialekt:

m ... Microsoft SQL-Server 2022 oder 2025 (inkl. Express)

o19 ... Oracle 19 (oder neuere Version)

Aktion:

u ... Update der Datenbankstruktur

Beispiel 1:

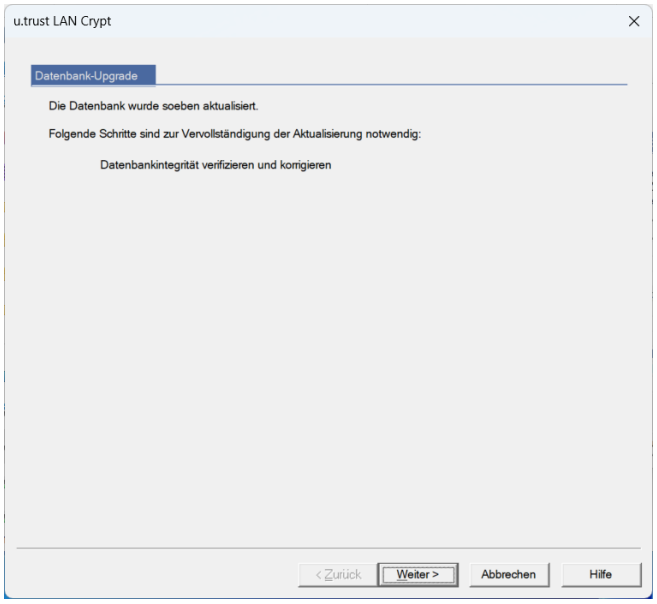
```
CreateTables SGLCSQLServer.dbo m u
```

Beispiel 2:

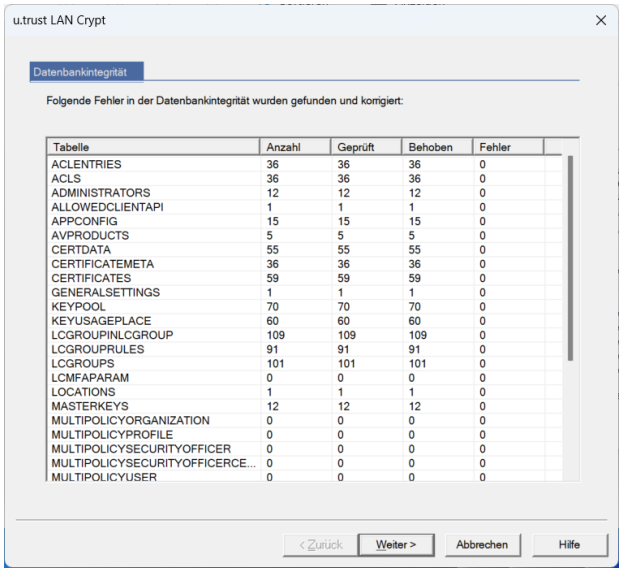
```
CreateTables SGLCSQLServer.SGLC o19 u
```

2.4.3 Upgrade-Assistent

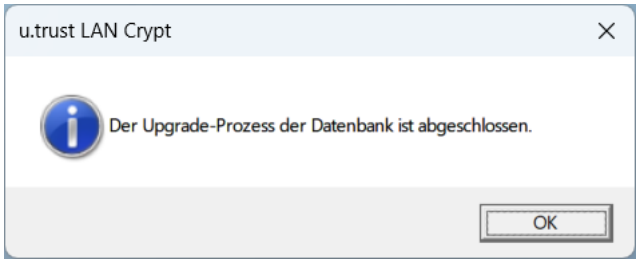
Nach dem Upgrade der Datenbank führt Sie ein *Upgrade-Assistent* durch die für das Abschließen des Upgrades erforderlichen Schritte. Dieser Assistent wird nach der ersten Anmeldung eines Master Security Officers an der aktualisierten Administration gestartet.



Hinweis: Nur ein Master Security Officer ist nach einem Upgrade zur ersten Anmeldung an der *u.trust LAN Crypt* Administration berechtigt. Wenn Sie nicht über die erforderlichen Rechte verfügen, wird eine entsprechende Meldung angezeigt. Die für das Abschließen des Upgrades notwendigen Schritte können je nach Version, von der das Upgrade durchgeführt wird, variieren.



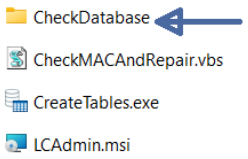
Der Upgrade-Assistent prüft die Integrität der *LAN Crypt* Datenbank und führt, wenn erforderlich, eine Fehlerbehebung durch. Im Anschluss werden Informationen zu allen korrigierten Fehlern angezeigt und ggf. weitere Maßnahmen empfohlen.



Nach Beenden des Assistenten steht die Administration wieder allen Security Officern zur Verfügung.

2.4.4 Integrität der Datenbank überprüfen und reparieren

Mithilfe des Kommandozeilen-Tools `CheckDatabase.exe` können Sie jederzeit die Integrität der Datenbank von *u.trust LAN Crypt* überprüfen und falls erforderlich eine Fehlerbehebung durchführen. Sie finden das Tool im *\Install-Ordner* Ihres *u.trust LAN Crypt* Installationspakets.



Hinweis: Eine detaillierte Beschreibung des Tools *CheckDatabase.exe* finden Sie unter: https://help.lancrypt.com/docs/admin/additional-documentation/CheckDatabaseTool/de/

2.5 Spracheinstellungen

u.trust LAN Crypt Administration unterstützt aktuell folgende Sprachen:

- deutsch
- englisch
- französisch
- japanisch

Die Spracheinstellung von *u.trust LAN Crypt* richtet sich nach der jeweils aktuell eingestellten Spracheinstellung von Windows. Bei nicht unterstützten Sprachen, zeigt *u.trust LAN Crypt* die Dialoge standardmäßig in englischer Sprache an.

Alternativ können Sie die Sprache für *u.trust LAN Crypt* aber auch selbst festlegen. Führen Sie hierzu in der Registry des Rechners, auf dem *u.trust LAN Crypt* Administration installiert ist, folgende Änderungen durch:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Utimaco\SGLANG]
"LCID"=dword:0x0407
```

für deutsche Sprache

```
"LCID"=dword:0x0409
```

für englische Sprache (US)

```
"LCID"=dword:0x040C
```

für französische Sprache

```
"LCID"=dword:0x0411
```

für japanische Sprache

Starten Sie danach den Rechner neu.

Die manuell eingestellte Sprache für *u.trust LAN Crypt* bleibt erhalten, auch wenn in Windows eine andere Sprache eingestellt ist oder diese geändert wird.

2.6 Deinstallation

Hinweis: Die Deinstallation von *u.trust LAN Crypt* ist nur möglich, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind.

1. Klicken Sie auf **Start**, **Einstellungen**, **Apps**.
2. Wählen Sie aus der Liste der installierten Programme **u.trust LAN Crypt Administration**.
3. Klicken Sie auf **Deinstallieren**, um *u.trust LAN Crypt* Administration zu deinstallieren.
4. Bestätigen Sie den Warnhinweis mit **OK**, wenn Sie *u.trust LAN Crypt* Administration tatsächlich deinstallieren möchten.
5. Führen Sie einen **Neustart** des Systems aus, um die Deinstallation abzuschließen.

Hinweis: Bei der Deinstallation von *u.trust LAN Crypt* bleibt der Inhalt der *u.trust LAN Crypt* Datenbank erhalten. Diese muss bei Bedarf gesondert mit Mitteln des Betriebssystems bzw. des Datenbankadministrationswerkzeugs gelöscht werden.

3 Administration

Die *u.trust LAN Crypt* Administration fügt sich nahtlos in Microsofts Management Konsole (MMC) ein und bietet einem Security Officer eine vertraute Benutzerschnittstelle mit den typischen MMC-Funktionen.

Die Administration wurde entwickelt, um die Vorteile bestehender Windows Replikationsmechanismen nutzen zu können. Dies ermöglicht eine sehr hohe Effizienz und die Reduktion der Gesamtkosten (TCO), da Kunden, die viele Arbeitsstationen zu verwalten haben, in der Regel nur ein System zur Verwaltung ihrer Arbeitsstationen einsetzen wollen.

Die Administration von *u.trust LAN Crypt* findet üblicherweise auf einem eigenen Administrationsrechner statt, von dem aus auf die benötigten Verzeichnisdienste (z. B. das Active Directory) und auf die *u.trust LAN Crypt* Datenbank zugegriffen wird.

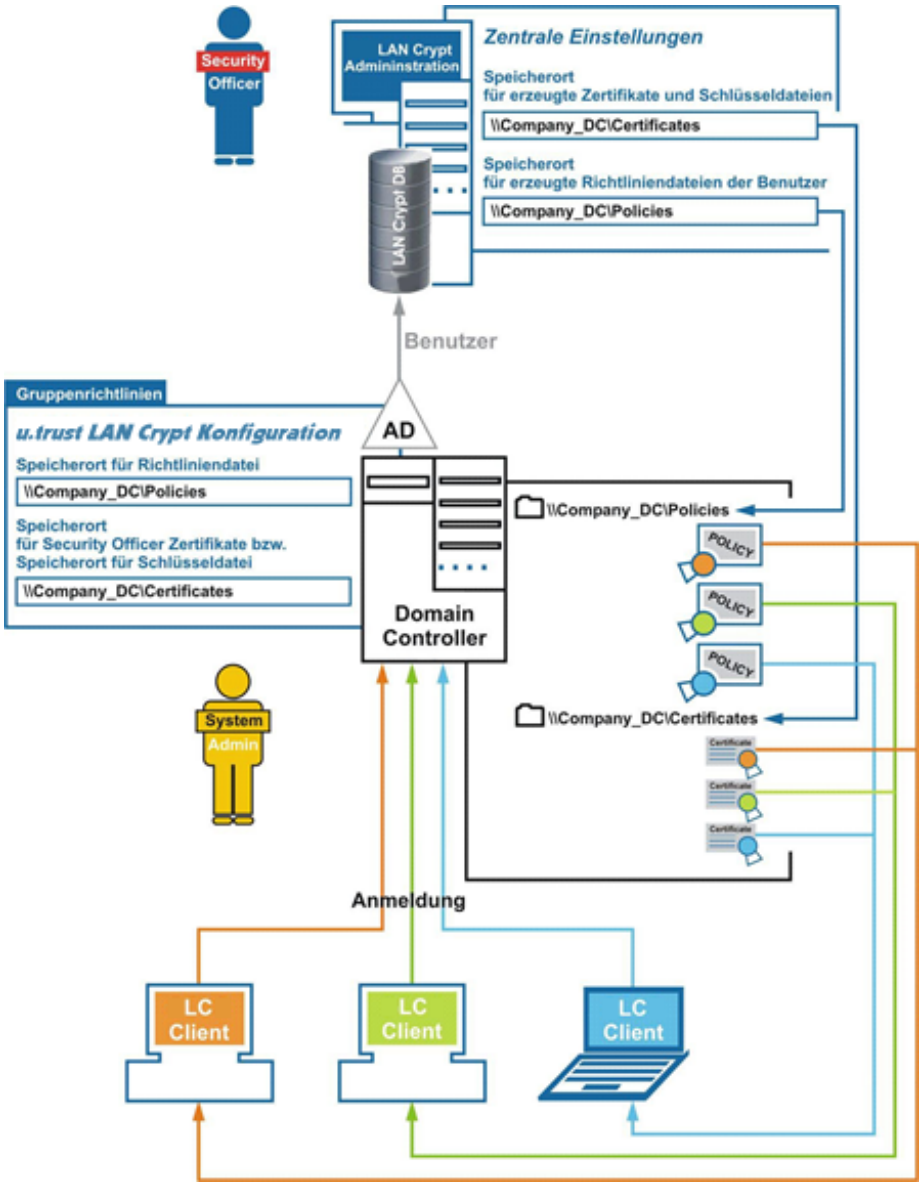
u.trust LAN Crypt verwendet das Security Officer-Konzept. Zu Beginn steht ein **Master Security Officer**, der die *u.trust LAN Crypt* Admin-Konsole installiert. Bei der Installation können bereits die Speicherorte für die von *u.trust LAN Crypt* erzeugten Zertifikate und Schlüsseldateien angegeben werden. Nachdem die *u.trust LAN Crypt* Admin-Konsole installiert ist, können Sie über diese auch noch den Speicherort für die Profildateien der Benutzer definieren. Sobald ein Security Officer einem Benutzer ein Profil zuweist, wird es dort gespeichert. Über Profile erhalten Benutzer ihre Verschlüsselungsinformationen.

Die Zertifikate, Schlüsseldateien („.p12“-Dateien) und Profildateien werden später von den *u.trust LAN Crypt* Clients automatisch aus den angegebenen Verzeichnissen importiert.

Dazu ist es notwendig, dass die Clients Zugriff auf diese Verzeichnisse haben. Aus diesem Grund definieren **Master Security Officer** und **Systemadministrator** gemeinsam Verzeichnisse, in denen diese Dateien gespeichert werden (typischerweise sind dies freigegebene Netzwerk-Shares).

Die Information, an welchen Speicherorten sich diese Dateien befinden, erhalten die Clients über Gruppenrichtlinien bei der Anmeldung an einen Domänencontroller. Die Speicherorte der Dateien müssen vom Systemadministrator in der *u.trust LAN Crypt* Konfiguration (siehe Abschnitt 4.1 „*u.trust LAN Crypt Konfiguration, Client-Einstellungen*“ auf Seite 177) eingetragen werden.

Die *u.trust LAN Crypt* Konfiguration wird in der für die Benutzer gültigen Gruppenrichtlinie vorgenommen.



Die *u.trust LAN Crypt* Clients benötigen keine Verbindung zur *u.trust LAN Crypt* Datenbank. Bei der Anmeldung erhalten diese über Gruppenrichtlinien (siehe Abschnitt 4.1 „Client-Einstellungen“) die erforderliche Information, unter welchem Pfad die jeweiligen *Zertifikate*, *Schlüsseldateien („.p12“-Dateien)* sowie *Profildateien* („*.xml.bz2“-Dateien*) zu finden sind. Danach werden diese Dateien automatisch auf die Clients übertragen.

Für den Import ihres Zertifikats benötigt der Benutzer eine PIN. Bei durch *u.trust LAN Crypt* erzeugten Zertifikaten wird die hierfür erforderliche PIN in der Datei *p12pwlog.csv* gespeichert. Dieses kann z. B. auch über PIN-Mailer (z. B. mithilfe des mitgelieferten Tools „*LCSendP12Password*“) an die Benutzer verteilt werden. Den Pfad der Passwortprotokolldatei definiert der Security Officer über den Knoten **Zentrale Einstellungen** unter dem Reiter **Verzeichnisse** innerhalb der *u.trust LAN Crypt* Administration.

3.1 Notwendige Schritte

Vorarbeiten:

- Optional: Installation des DBMS (Microsoft oder Oracle). Erzeugen einer neuen Datenbank „LANCRYPT“. Die in den DBMS vorangestellten Datenbanken sollten nicht *für u.trust LAN Crypt* benutzt werden!
- Datenquelle (32 Bit ODBC) als System-DSN hinzufügen (siehe Abschnitt 3.2.2)
- Datenbanktabellen mit `CreateTables` erzeugen (oder bei einem Upgrade erweitern)
- Systemadministrator: Einstellungen in der *u.trust LAN Crypt* Konfiguration vornehmen.
- Initialen Master Security Officer anlegen
- Angaben der Speicherorte in der Admin-Konsole:
  - für von *u.trust LAN Crypt* erzeugte Security Officer Zertifikate.
  - für die Passwortprotokolldatei der automatisch generierten Passwörter der Schlüsseldateien (nur, wenn die Zertifikate von *u.trust LAN Crypt* erzeugt werden).
  - für von *u.trust LAN Crypt* erzeugte Profildateien (sprechen Sie sich mit dem System-Administrator ab, um diese Schritte umzusetzen)

Hinweis: Bei der Verwendung von Oracle-Datenbanken sollten, wenn von verschiedenen Administrationsstationen auf die Datenbank zugegriffen wird, jetzt auch die Code Page-Einstellungen vorgenommen werden (siehe „*Datenbank*“ auf Seite 79).

- weitere Security Officer anlegen
- Rechte für die Security Officer definieren
- Objekte (Organisationseinheiten, Gruppen, Benutzer) aus dem Verzeichnisdienst (z. B. Active Directory) importieren
- *u.trust LAN Crypt* Gruppen erstellen und mit den aus dem Verzeichnisdienst importierten Objekten füllen (Anwender, Gruppen)
- den einzelnen Organisationseinheiten bzw. Regionen die *u.trust LAN Crypt* Gruppen und den jeweils hierfür zuständigen Security Officer zuordnen sowie deren Rechte festlegen
- Schlüssel anlegen
- Verschlüsselungsregeln anlegen

  Hinweis: Wir empfehlen, Verschlüsselungsregeln nur in *LAN Crypt* Gruppen zu definieren. Verschlüsselungsregeln in direkt importierten Verzeichnisobjekten stellen ein Sicherheitsrisiko dar und sind zudem fehleranfällig.

- Zertifikate für die Benutzer erzeugen bzw. diesen zuweisen
- Profildateien für die Benutzer erzeugen

3.2 Vorarbeiten für die Administration von u.trust LAN Crypt

Nach der Installation sind folgende Schritte notwendig, bevor Sie mit der Administration von *u.trust LAN Crypt* beginnen können:

- Optional: Datenbankverwaltungssystem installieren

Dies ist nur notwendig, wenn Sie nicht selbst über ein Datenbanksystem verfügen, aus dem Sie eine Datenbank für die Administration von *u.trust LAN Crypt* verwenden wollen.

u.trust LAN Crypt Version 13.0.1 unterstützt folgende Datenbanksysteme:

- Microsoft SQL-Server 2022 oder 2025 (inkl. Express)
- Oracle *19 (*oder neuere Version)

  Hinweis: Kommt eine Oracle-Datenbank zum Einsatz, ist für die *u.trust LAN Crypt* Administration die Installation eines Oracle-Client notwendig. Bei Wahl der Oracle Client-variante „Laufzeit“ ist die Installation des **Oracle ODBC-Treibers** erforderlich.

  Microsoft ODBC für Oracle wird von *u.trust LAN Crypt* nicht unterstützt.

  Achten Sie auch darauf, dass Sie bei der Erzeugung von Datenbankobjekten keine vom jeweiligen Hersteller reservierten Schlüsselwörter verwenden.

- Datenquelle angeben (ODBC)

  Wenn Sie ein eigenes Datenbanksystem verwenden, müssen Sie die Zugangsdaten für die entsprechende Datenbank für die Angabe der Datenquelle kennen.

- Datenbanktabellen erzeugen

  Nach Angabe der Datenquelle müssen Sie mit einem mitgelieferten Tool (`CreateTables.exe`) die *u.trust LAN Crypt* Tabellen in der *LAN Crypt* Datenbank erzeugen.

  SQL-Dialekt:

  m ... Microsoft SQL-Server 2022 oder 2025 (inkl. Express)

  o19 ... Oracle 19 (oder neuere Version)

  Aktion:

  c ... Erzeuge alle Tabellen

  Beispiel 1:

  ```
  CreateTables SGLCSQLServer.dbo m c
  ```

  Beispiel 2:

  ```
  CreateTables SGLCSQLServer.SGLC o19 c
  ```

3.2.1 Installation des Datenbanksystems

Die folgende Beschreibung bezieht sich auf die *Microsoft SQL-Server 2022 Express Edition*. Für diese beispielhafte Beschreibung werden so weit wie möglich die Voreinstellungen dieser Version verwendet.

Gehen Sie für die Installation des Datenbanksystems folgendermaßen vor:

1. Laden Sie eine aktuelle Version von Microsoft SQL-Server Express (z. B. Microsoft SQL-Server 2022 Express) von der Microsoft Webseite herunter. Doppelklicken Sie dann im Downloadordner auf die Installationsdatei. Bei Microsoft SQL-Server 2022 Express ist dies *SQL2022-SSEI-Expr.exe*.

   Hinweis: Laden Sie bitte eine 64-Bit-Version von Microsoft SQL-Server Express Edition von *www.microsoft.com* herunter.

   Akzeptieren Sie die Lizenzbestimmungen und klicken Sie auf **Weiter**.

2. Die Installationsdateien werden extrahiert und ein Installationsassistent wird gestartet.

3. Folgen Sie den Anweisungen des Installationsassistenten und übernehmen Sie alle Voreinstellungen.

   Voreinstellungen: Die folgenden Beschreibungen der Vorarbeiten beziehen sich auf diese Voreinstellungen. Sollten Sie Änderungen vornehmen (Authentisierungsmethode, Datenbankinstanz) müssen Sie diese bei der Angabe der Datenquelle und dem Erzeugen der Datenbanktabellen berücksichtigen.

   Datenbankauthentisierung: Standardmäßig arbeitet die Express Edition mit Windows Authentisierung. Diese wiederum setzt voraus, dass der Benutzer, der sich an der Datenbank anmeldet, über Windows-Administratorrechte verfügt.

   Master-Datenbank: Standardmäßig wird bei der Angabe der Datenquelle die vorhandene Master-Datenbank verwendet. Im Allgemeinen empfehlen wir, NICHT die Master-Datenbank zu verwenden, da diese beim Upgrade der Express Edition oder der SQL-Server Version unter Umständen Probleme verursacht.

   Sie können eine separate Datenbank für *u.trust LAN Crypt* erstellen (z. B. „LANCrypt“) und diese beim Hinzufügen der Datenquelle angeben. Für die Microsoft SQL-Server 2022 Express Edition können Sie mit dem folgenden Kommando auf der Kommandozeile eine Datenbank erstellen:

   ```
   osql -E -S .\SQLEXPRESS -Q "CREATE DATABASE <Name_der_Datenbank>"
   ```

   Es wird eine Datenbank mit dem angegebenen Namen und mit Windows-Authentisierung erstellt.

   Mit dem Parameter `-U` können Sie zum Beispiel einen Benutzernamen für die Authentisierung angeben. Um alle Parameter anzeigen zu lassen, geben Sie `osql -?` ein.

   u.trust LAN Crypt unterstützt Microsoft SQL-Server Express. Das Programm steht kostenlos zur Verfügung und kann zum Erstellen einer separaten Datenbank verwendet werden.

Ebenso können Sie Microsoft SQL-Server Management Studio Express herunterladen. Auch dieses Programm steht kostenlos zur Verfügung und kann zum Erstellen einer separaten Datenbank verwendet werden.

Im nächsten Schritt muss eine Datenquelle angegeben werden, damit *u.trust LAN Crypt* das Datenbanksystem benutzen kann.

3.2.2 Datenquelle (ODBC) hinzufügen

Hinweis: Die Datenquelle muss mit dem *32-Bit ODBC Data Source Administrator* hinzugefügt werden. Dieser ist auch bei 64-Bit-Systemen verfügbar. Starten Sie den *ODBC Data Source Administrator* über das Windows Startmenü im Abschnitt *Windows-Verwaltungsprogramme* und wählen dort *ODBC Data Sources (32 Bit)*. Damit stellen Sie sicher, dass die richtige Version gestartet wird. Es steht hierzu auch ein Link über das Windows Startmenü unter **u.trust LAN Crypt Administration** zur Verfügung.

Damit *u.trust LAN Crypt* die Datenbank über das Datenverwaltungssystem verwenden kann, muss dem System die Datenquelle mitgeteilt werden. Dies erfolgt über den ODBC-Datenquellen-Administrator.

ODBC (Open Database Connectivity) ermöglicht den Zugriff auf Daten aus den unterschiedlichsten Datenbankverwaltungssystemen. Verfügen Sie beispielsweise über ein Programm für den Zugriff auf Daten in einer SQL-Datenbank, bietet Ihnen ODBC die Möglichkeit, mit demselben Programm auf Daten in einer anderen Datenbank zuzugreifen. Hierzu müssen Sie mit den System-Softwarekomponenten den sogenannten Treiber hinzufügen. ODBC unterstützt Sie beim Hinzufügen und Konfigurieren dieser Treiber.

Zum Hinzufügen der Datenquelle:

1. Klicken Sie auf *Start\Windows-Verwaltungsprogramme\ODBC Data Sources (32 Bit)*. Der ODBC-Datenquellen-Administrator wird gestartet.
2. Wählen Sie den Reiter **System-DSN** aus und klicken Sie auf **Hinzufügen**.

   Über diesen Reiter werden Datenquellen mit System-Datenquellennamen (DSN) hinzugefügt. Diese Datenquellen sind lokal auf einem Computer gespeichert, jedoch nicht einem bestimmten Benutzer zugewiesen; jeder Benutzer mit entsprechenden Berechtigungen kann einen System-DSN verwenden.
3. Wählen Sie als Treiber, für den Sie die Datenquelle erstellen wollen, **SQL-Server** aus und klicken Sie auf **Fertigstellen**.

   Hinweis: Wenn SQL-Server Native Client in der Liste verfügbar ist, wählen Sie diesen Eintrag aus. Zur Absicherung der Verbindung zwischen der *u.trust LAN Crypt Administration* und dem SQL-Server empfehlen wir, „*ODBC Driver 17 for SQL-Server*“ oder eine neuere Version zu verwenden. Dieser Treiber erlaubt eine Verbindungsverschlüsselung mit TLS 1.2 und bietet damit eine erhöhte Sicherheit. Ein Download ist möglich über: https://go.microsoft.com/fwlink/?linkid=2120137
4. Geben Sie im nächsten Dialog als Namen, mit dem Sie auf die Datenquelle verweisen wollen, **SGLCSQLServer** ein.

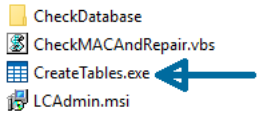
Der Name für den Verweis auf die Datenquelle ist in der *u.trust LAN Crypt* Konfiguration einstellbar. In der Standardeinstellung wird **SGLCSQLServer** verwendet. Wenn Sie einen anderen Namen verwenden wollen, muss dieser in der Konfiguration angegeben werden (siehe Abschnitt 4.2.4 „*ODBC-Datenquelle*“).

Hinweis: Der Name der ODBC-Quelle unterscheidet nach Groß-/Kleinschreibung! Er muss hier genauso angegeben werden, wie er in der *u.trust LAN Crypt* Konfiguration angegeben wird. Sie müssen den Namen in der Konfiguration angeben, bevor die *u.trust LAN Crypt* Administration das erste Mal gestartet wird.

5. Wählen Sie unter *Server* aus, mit welchem Server die Verbindung hergestellt werden soll, und klicken Sie auf **Weiter**.
6. Verwenden Sie im nächsten Dialog die Standardeinstellungen. Durch die Wahl der Option **Mit Windows NT-Authentifizierung anhand des Benutzernamens im Netzwerk** werden die Windows Benutzerdaten zur Anmeldung an das Datenbanksystem verwendet. Eine Eingabe des Passwortes ist nicht erforderlich. Klicken Sie auf **Weiter**.
7. Wählen Sie als Standarddatenbank die Datenbank (z. B. LANCrypt), die Sie für *u.trust LAN Crypt* erzeugt haben, und bestätigen Sie diese.
8. Belassen Sie im nächsten Dialog die Standardeinstellungen und klicken Sie auf **Fertigstellen**.

3.2.3 Tabellen in der u.trust LAN Crypt Datenbank erzeugen

Mit dem Kommandozeilen-Tool `CreateTables.exe` können Sie die erforderlichen Tabellen in Ihrer *u.trust LAN Crypt*-Datenbank anlegen. Sie finden das Tool im Installations-Verzeichnis Ihres extrahierten Installationspakets.



Hinweis: Die Anmeldung an der Datenbank muss mit Berechtigungen erfolgen, die das Erzeugen und Ändern des Datenbankschemas ermöglichen.

So erzeugen Sie die Tabellen in Ihrer Datenbank:

Geben Sie auf der Kommandozeile, wenn Sie Microsoft SQL-Server (inkl. Express) verwenden, Folgendes ein: `CreateTables SGLCSQLServer.dbo m c`.

Wenn Sie die Installation mit den Voreinstellungen erfolgreich vorgenommen haben, ist das Datenbanksystem nun fertig konfiguriert. Sie können nun die *u.trust LAN Crypt* Administration starten.

3.2.3.1 CreateTables Kommandozeilensyntax

```
CreateTables <ODBCName[.Besitzer-Name]> <SQL-Dialekt> <Aktion>
```

`CreateTables.exe` verfügt für das Erzeugen der Tabellen in unterschiedlichen Konfigurationen über folgende Parameter:

ODBCName:

Der Name, den Sie für die ODBC- Datenquelle verwendet haben.

Datenbankbesitzer Name

Damit die Datenbank korrekt angesprochen werden kann, muss für Oracle-Datenbanken der Datenbankbesitzer angegeben werden. Der Besitzer der Datenbank muss unbedingt in GROSSBUCHSTABEN angegeben werden. Falls das Standard-Schema Ihres Microsoft SQL-Servers nicht *.dbo* entspricht, müssen Sie für Microsoft SQL-Datenbanken den Datenbankbesitzer *.dbo* mit angeben.

SQL-Dialekt:

m ... Microsoft SQL-Server 2022 oder 2025 (inkl. Express)

o19 ... Oracle 19 (oder neuere Version)

Aktionen:

c ... Alle Tabellen erzeugen (nur Neuinstallation)

u … Alle Tabellen aktualisieren (nur Upgrade)

Beispiel 1 (bei Neuinstallation):

```
CreateTables SGLCSQLServer.dbo m c
CreateTables SGLCSQLServer.SGLC o19 c
```

Beispiel 2 (bei Upgrade):

```
CreateTables SGLCSQLServer.dbo m u
CreateTables SGLCSQLServer.SGLC o19 u
```

3.3 Master Security Officer

u.trust LAN Crypt verwendet das Security Officer-Konzept. Am Beginn steht ein Master Security Officer, der in weiterer Folge Aufgaben delegieren kann, indem er weitere Security Officer (eventuell auch weitere Master Security Officer) anlegt und diese mit bestimmten Rechten für die Administration von *u.trust LAN Crypt* ausstattet. Der zuerst angelegte Master Security Officer kann zusätzliche Security Officer anlegen.

Die Rechte der von einem Master Security Officer angelegten Security Officer, werden über ACLs definiert. Die einzelnen Security Officer können dann verschiedenen Organisationseinheiten in der zentralen Administration zugeordnet werden. Deren Rechte beziehen sich dann ausschließlich auf die Organisationseinheit, der sie zugeordnet wurden. Diese Rechte werden in der Organisationshierarchie nach unten weitervererbt, bis an einem Punkt andere Rechte festgelegt werden.

Nachdem das Datenbanksystem und die Datenquelle vorbereitet wurden, wird beim ersten Starten der Administration von *u.trust LAN Crypt*, ein initialer **Master Security Officer** angelegt.

Ein Master Security Officer ist immer mit allen zur Verfügung stehenden Rechten ausgestattet.

Hinweis: Beim Anlegen dieses initialen Master Security Officers wird auch der Speicherort für von *u.trust LAN Crypt* erzeugte Zertifikate und Schlüsseldateien angegeben. Dort wird auch der öffentliche Teil des Security Officer Zertifikats gespeichert, der von den Clients benötigt wird. Aus diesem Verzeichnis werden später auch die Benutzerzertifikate (*.p12*-Dateien) von den Clients importiert. Das Verzeichnis (Netzwerk-Share), das Sie gemeinsam mit dem **System Administrator** definiert haben, sollte nun verfügbar sein.

Alle Einstellungen, die Sie beim Anlegen des initialen Master Security Officers vornehmen, können Sie später in der *u.trust LAN Crypt* Administration unter dem Hauptknoten **Zentrale Einstellungen** ändern.

3.3.1 Initialer Master Security Officer

Nach dem ersten Start der *u.trust LAN Crypt* Admin-Konsole (*C:\Programme (x86)\Utimaco\u.trust LAN Crypt\Administration\SGLCAdmin.msc*) wird nach der Anmeldung an die Datenbank der Assistent zum Anlegen des initialen Master Security Officers angezeigt.

Geben Sie im ersten Dialog des Assistenten die Daten für den initialen Master Security Officer ein. Der hier eingetragene Name wird als *Common Name* im Zertifikat eingetragen, wenn Sie von *u.trust LAN Crypt* erzeugte Zertifikate verwenden. E-Mail-Adresse und Kommentar sind jeweils optional. Klicken Sie auf **Weiter**.

Hinweis: Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von *u.trust LAN Crypt* erzeugte Zertifikate eingetragen. Sie kann z. B. auch für die Erstellung eines PIN-Mailers (z. B: mithilfe von *„LCSendP12Password“)* via E-Mail verwendet werden.

Im zweiten Dialog des Assistenten werden die Speicherorte für

- erzeugte Zertifikate und Schlüsseldateien (*.p12*),
- für erzeugte Security Officer Zertifikate und
- die Protokolldatei für automatisch generierte Passwörter der erzeugten Schlüsseldateien angegeben.

Speicherort für erzeugte Zertifikate und Schlüsseldateien

u.trust LAN Crypt kann bei Bedarf selbst-signierte Zertifikate erzeugen. Die hierbei erzeugten Schlüsseldateien (*.p12*) für die Benutzer enthalten neben den Zertifikaten auch die privaten Schlüssel. Diese werden bei der Zuweisung der Zertifikate für die Benutzer erzeugt. Der dazugehörige Speicherort ist im zweiten Dialog des Assistenten anzugeben. Typischerweise ist dies eine Netzwerkfreigabe, über die diese Dateien den Benutzern bereitgestellt werden.

Auch der öffentliche Teil des Security Officer Zertifikats (*.cer*) wird hier gespeichert.

Den Benutzern müssen ihre Schlüsseldateien bzw. Zertifikate (*.p12*), Profildateien und der öffentliche Teil des Zertifikats *(.cer-Datei*) desjenigen Security Officers, der die Profildateien erzeugt und signiert hat, zur Verfügung gestellt werden.

Dies erfolgt für die *u.trust LAN Crypt Client* Konfiguration mithilfe von Gruppenrichtlinien oder Registry-Einstellungen (falls kein Active Directory vorhanden ist oder aus Sicherheitsgründen nicht genutzt werden soll). Über diese Einstellungen bekommt der Client die passenden Zugriffspfade mitgeteilt. Wir empfehlen die Verwendung von UNC-Pfaden und von FQD-Namen (z. B. „*fileserver1.lancrypt.intern**freigabe**lcpolicies*").

Wird eine entsprechende „*.cer*"-Datei gefunden, die den öffentlichen Schlüssel des Security Officer Zertifikats enthält, wird diese automatisch importiert.

Hinweis: Um die beschriebene Funktionalität zu verwenden, müssen die entsprechenden Pfade in der *u.trust LAN Crypt* Gruppenrichtline konfiguriert oder in der Registry gesetzt sein.

Alternativ können die Schlüsseldateien der Benutzer und der öffentliche Teil des Security Officer Zertifikats auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide von den Clients importiert werden.

Hinweis: Auf den Clients muss immer der öffentliche Teil des Zertifikats jenes Security Officers importiert werden, von dem die Profildateien erzeugt werden.

Wird der Pfad, unter dem die öffentlichen Zertifikate (*.cer)* der Security Officer und die Schlüsseldateien (*.p12)* der Benutzer gespeichert werden, beispielsweise nach dem Anlegen weiterer Security Officer geändert, müssen diese Dateien in den neuen Pfad bzw. Ordner kopiert werden. Die öffentlichen Zertifikate der Security Officer können andernfalls nicht mehr von den *u.trust LAN Crypt* Clients gefunden werden. Die Schlüsseldateien der Benutzer müssen dann ebenfalls unter dem „neuen" Pfad für die Benutzer verfügbar sein.

Speicherort für erzeugte Security Officer Zertifikate

u.trust LAN Crypt speichert, z. B. für Backup-Zwecke, Security Officer Zertifikate in „.p12"-Dateien. Der Pfad bzw. Ordner, in dem diese Zertifikate gespeichert werden, kann hier angegeben werden.

Hinweis: Da es sich hierbei um sensible Daten handelt, müssen diese unbedingt vor unberechtigtem Zugriff geschützt werden!

Datei für Passwortprotokoll

Hier können Speicherort und Name für die Passwortprotokolldatei der generierten PKCS#12 Dateien angegeben werden (Standardname: *p12pwlog.csv*). Diese Datei enthält die Passwörter der erzeugten PKCS#12-Dateien (*.p12*). Diese kann z. B. auch für die Erstellung eines PIN-Briefs oder PIN-Mailers (z. B. mithilfe von „*LCSendP12Password*") verwendet werden.

Hinweis: Diese Datei sollte besonders geschützt werden und unter keinen Umständen im gleichen Speicherort wie die Profildateien oder Benutzerzertifikate gespeichert werden!

Mit *u.trust LAN Crypt* können Sie die Passwortprotokolldatei auf einfache Art und Weise schützen. Installieren Sie hierzu die *u.trust LAN Crypt* Komponenten *Admin-Konsole* und *Clientanwendung* auf demselben Computer. Erstellen Sie nach dem Anlegen des initialen Master Security Officers eine *Verschlüsselungsregel*, mit der die *Passwortprotokolldatei* verschlüsselt wird. Hierzu erzeugen Sie ein Profil für den ersten Master Security Officer (MSO) und laden Sie danach das Profil. Der verwendete Verschlüsselungsschlüssel sollte dabei ausschließlich dem Master Security Officer und den Security Officern zur Verfügung stehen, die das Recht besitzen, Zertifikate zu erzeugen. Durch das Erzeugen von zusätzlichen Regionen lassen sich auch voneinander getrennte Passwortprotokolldateien anlegen.

Hinweis: Wenn Sie beide *u.trust LAN Crypt* Komponenten, *Admin-Konsole* und *Clientanwendung* auf demselben Computer installieren, müssen diese **unbedingt** von der gleichen Version sein.

Durch Ausführen des Assistenten zur Initialverschlüsselung wird die *Passwortprotokolldatei* verschlüsselt und kann fortan von unautorisierten Personen nicht mehr eingesehen werden. Um sicherzustellen, dass das Passwort für den initialen Master Security Officer nicht manipuliert wurde, als die Datei noch nicht verschlüsselt war, erstellen Sie ein neues Zertifikat und weisen Sie es dem initialen Master Security Officer zu.

Hinweis: Wenn der Security Officer, der die Zertifikatszuordnung durchführt, im Dateisystem nicht das Recht hat, die Passwortprotokolldatei zu ändern, können keine *u.trust LAN Crypt* Zertifikate erzeugt werden.

Klicken Sie auf **Weiter**.

Zertifikatsgültigkeit

Im dritten Dialog des Assistenten können Sie die Gültigkeitsdauer für die von *u.trust LAN Crypt* erzeugten Zertifikate angeben und dem Security Officer ein bereits existierendes oder ein neues von *u.trust LAN Crypt* erzeugtes Zertifikat zuweisen.

Wenn Sie zur Sicherung der Daten dieses Security Officers ein von *u.trust LAN Crypt* erzeugtes Zertifikat verwenden, wird es mit der hier angegebenen Gültigkeitsdauer erzeugt. Auch alle weiteren mit u.trust LAN Crypt neu erzeugten Zertifikate erhalten dann ebenfalls diese Gültigkeitsdauer.

Zertifikat des initialen Security Officers

Sie müssen ein Verschlüsselungszertifikat auswählen, mit dem die Daten des Security Officers gesichert werden. Optional können Sie zusätzlich ein separates Signaturzertifikat auswählen, mit dem der Security Officer die Profildateien signieren soll. Geben Sie ein solches separates Signaturzertifikat nicht an, dient das Verschlüsselungszertifikat auch zur Signierung der Profildateien.

Klicken Sie auf die Schaltfläche **Suchen**, um im folgenden Dialog ein bestehendes Zertifikat auszuwählen. Klicken Sie in diesem Dialog auf die Schaltfläche **Neues Zertifikat**, wenn *u.trust LAN Crypt* ein neues Zertifikat erzeugen soll.

Hinweis: Wenn Sie ein bereits vorhandenes Zertifikat verwenden wollen, müssen Sie dieses jetzt zur Verfügung haben. Falls Sie mit einem Software-Zertifikat arbeiten, muss sich dieses

im Zertifikatsspeicher befinden. Ist das Zertifikat auf einem Token gespeichert, muss dieser mit dem System verbunden sein. Zum Importieren des Zertifikats klicken Sie auf die Schaltfläche **Zertifikat Importieren**.

Klicken Sie im angezeigten Dialog auf **Neues Zertifikat**. Wählen Sie das neue Zertifikat aus der Zertifikatsliste des ausgewählten Zertifikatsspeichers aus und klicken Sie auf **OK**.

Klicken Sie auf **Weiter**.

Im vierten Dialog des Assistenten können Sie optional eine Region mit einem entsprechenden Präfix angeben. Das Präfix wird beim Erzeugen der Schlüssel dem Schlüsselnamen vorangestellt. Es wird immer das Präfix jener Region verwendet, die dem Security Officer zugeteilt ist, der den Schlüssel erzeugt. Aufgrund des Präfixes ist dann immer eindeutig ersichtlich, für welche Administrationseinheit der Schlüssel verwendet werden soll. Über den Knoten **Zentrale Einstellungen** der Admin-Konsole können auch später noch weitere Regionen erstellt werden und dann den verschiedenen Security Officers zugeteilt werden. Diese Vorgehensweise ist speziell für verteilte Umgebungen vorgesehen.

Die Angabe eines Standorts ist immer zwingend. Der Standort wird benötigt, um bei der Protokollierung von *u.trust LAN Crypt* bei der Verwendung von verteilten Datenbanken die Einträge eindeutig zuordnen zu können.

Sie müssen auch dann einen Standort eintragen, wenn Sie keine verteilte Datenbank verwenden. Nur so stellen Sie sicher, dass Einträge eindeutig zugeordnet werden, falls die Datenbank später einmal auf verschiedene Standorte verteilt wird.

Nach dem Klicken auf **Fertigstellen** wird der initiale Master Security Officer angelegt und der Dialog zur Anmeldung an die *u.trust LAN Crypt* Administration wird angezeigt.

In diesem Dialog werden später alle Security Officer, die das Recht haben, sich an die *u.trust LAN Crypt* Administrationsdatenbank anzumelden, angezeigt.

Markieren Sie in diesem Dialog den neu angelegten Master Security Officer und klicken Sie auf **OK**. Die *u.trust LAN Crypt* Admin-Konsole wird geöffnet.

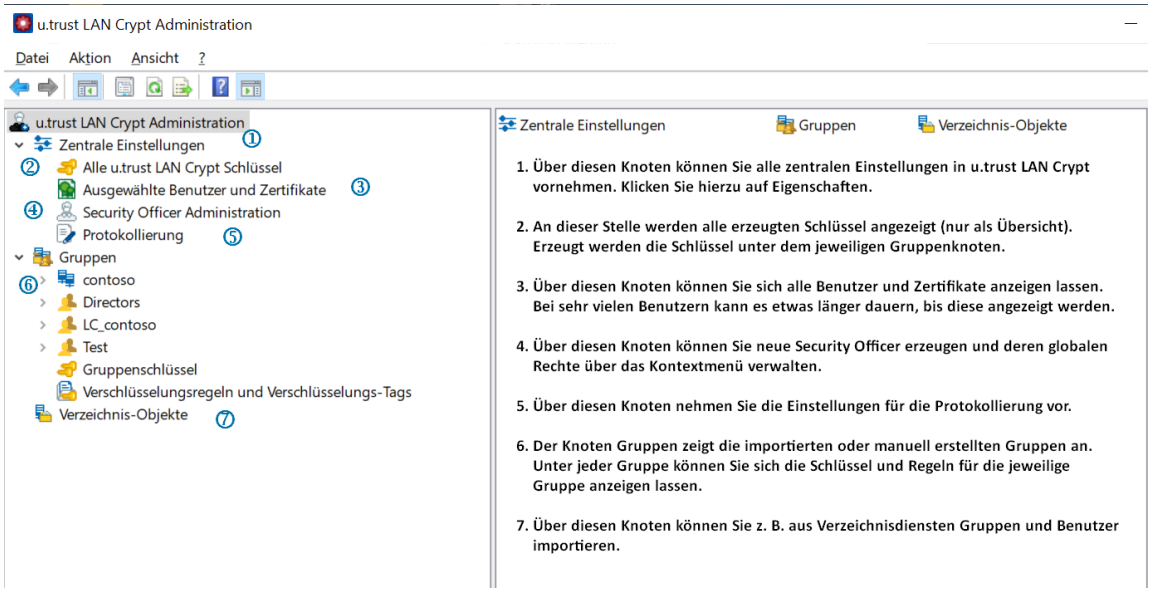
Hinweis: Nach der Anmeldung werden Sie in einem Dialog darauf hingewiesen, dass noch kein Wiederherstellungsschlüssel erzeugt wurde. Ohne einen Wiederherstellungsschlüssel ist in einem Notfall (z. B., wenn kein Zertifikat für die Anmeldung zur Verfügung steht, bzw. wenn dieses abgelaufen oder beschädigt ist) das Risiko eines vollständigen Datenverlustes sehr hoch.

Dieser Dialog wird bei der Anmeldung eines Master Security Officers angezeigt, bis ein Wiederherstellungsschlüssel erzeugt wurde. Durch Aktivieren der Option **Diese Warnung nicht mehr anzeigen** kann die Anzeige des Dialogs unterdrückt werden, auch wenn kein Wiederherstellungsschlüssel erzeugt wurde.

Hinweis: Um einen möglichen Datenverlust zu vermeiden, sollten Sie einen Wiederherstellungsschlüssel erzeugen.

3.4 Administration: Überblick

Bei der Installation von *u.trust LAN Crypt* wird die Datei **SGLCAdmin.msc** im Installationsverzeichnis von *u.trust LAN Crypt* angelegt. Über das Windows-Start-Menü (*u.trust LAN Crypt Administration / Administration*) kann durch Klicken auf diesen Eintrag ein Fenster der Management Konsole geöffnet werden, welches nur die für die Administration von *u.trust LAN Crypt* notwendigen Snap-Ins enthält.



Das Snap-In für die *u.trust LAN Crypt* Administration kann auch der Standardansicht der Management Konsole hinzugefügt werden (Datei / Snap-In hinzufügen / entfernen – *u.trust LAN Crypt* Administration). Beim Hinzufügen ist bereits das Passwort für die *u.trust LAN Crypt* Administrationsdatenbank notwendig.

Wer ist angemeldet?

In der Statuszeile wird der aktuell angemeldete Security Officer angezeigt. Außerdem sehen Sie, ob es sich um einen Master Security Officer (MSO) oder einen Security Officer (SO) handelt.

Symbolleiste in der Administration

u.trust LAN Crypt stellt für viele seiner Funktionen Symbole in der Symbolleiste der Management Konsole zur Verfügung. Art und Anzahl der Symbole in der Symbolleiste sind abhängig vom jeweils markierten Knoten.

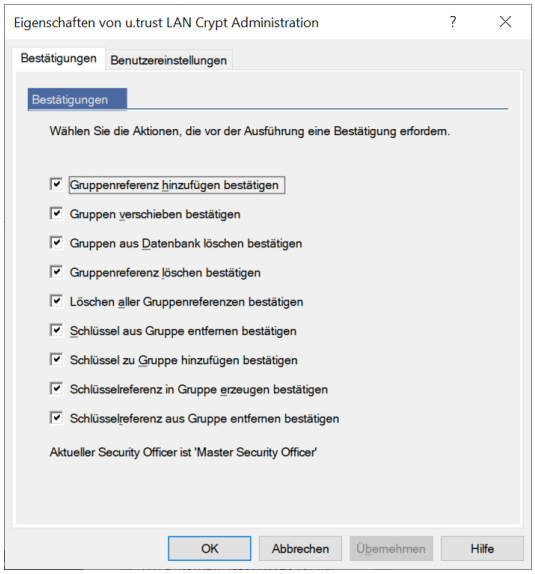
Alle Funktionen, die über diese Symbole auswählbar sind, können auch über das entsprechende Kontextmenü durchgeführt werden.

Über einen Klick mit der rechten Maustaste auf den Knoten **u.trust LAN Crypt Administration** können Sie sich die Eigenschaften des Knotens anzeigen lassen und diese bei Bedarf anpassen. Eine Beschreibung der Eigenschaften können Sie den folgenden Abschnitten entnehmen.

3.4.1 Bestätigungen

Sie haben in der *u.trust LAN Crypt* Administration die Möglichkeit einzustellen, welche Aktionen vor der eigentlichen Ausführung bestätigt werden müssen. Klicken Sie hierzu auf **Eigenschaften** im Kontextmenü des **u.trust LAN Crypt Administration** Basisknotens.

Der folgende Dialog zeigt die verfügbaren Aktionen an:



Wenn Sie hier eine Aktion markieren, muss diese vor ihrer Ausführung in einem Dialog zunächst bestätigt werden. Erst danach wird die Aktion auch ausgeführt.

Diese Einstellung können Sie für folgende Aktionen vornehmen:

- **Gruppenreferenz hinzufügen bestätigen**

  Das Hinzufügen einer Gruppenreferenz zu einer anderen Gruppe muss bestätigt werden. Gruppe markieren > rechte Maustaste > Kopieren > andere Gruppe auswählen > rechte Maustaste > Einfügen > Bestätigung

  Hinweis: Die Funktionen *Kopieren*; *Ausschneiden* und *Einfügen* sind sowohl über die Kontextmenüs als auch mit der Maus über „*Drag & Drop*“ oder „*Drag & Drop + STRG*“ möglich.

- **Gruppen verschieben bestätigen**

  Das Verschieben einer Gruppe in eine andere Gruppe muss bestätigt werden.

- **Gruppen aus Datenbank löschen bestätigen**

  Das Löschen einer Gruppe muss bestätigt werden.

- **Gruppenreferenz löschen bestätigen**

  Das Entfernen einer Gruppenreferenz (Shortcut) muss bestätigt werden.

- **Löschen aller Gruppenreferenzen bestätigen**

  Wenn es eine Referenz von einer Gruppe zu einer anderen Gruppe gibt, z.B. eine Verknüpfung von Gruppe 1 und Gruppe 2 in Gruppe 3, so muss das Löschen dieser Referenz bestätigt werden. (Gruppe 3 auswählen > rechte Maustaste > **Referenz entfernen** auswählen).

- **Schlüssel aus Gruppe entfernen bestätigen**

  Das Entfernen von Schlüsseln, die zuvor in einer Regel verwendet und anschließend deaktiviert wurden, muss bestätigt werden. Bereits verwendete Schlüssel sind in der Administration entsprechend markiert und verbleiben in der Datenbank, auch wenn sie aus der Gruppe entfernt werden. Schlüssel, die noch nicht verwendet wurden, werden beim Entfernen aus einer Gruppe auch aus der Datenbank gelöscht.

- **Schlüssel aus Gruppe hinzufügen bestätigen**

  Schlüssel, die in einer Regel verwendet und anschließend aus allen Gruppen entfernt wurden, verbleiben in der Datenbank und werden unter dem Knoten **Zentrale Einstellungen** > **Alle LAN Crypt-Schlüssel** angezeigt. Von dort können sie wieder über „*Drag & Drop“* einer Gruppe hinzugefügt werden. Diese Aktion muss bestätigt werden.

- **Schlüsselreferenz in Gruppe erzeugen bestätigen**

  Das Hinzufügen einer Schlüsselreferenz zu einer Gruppe (z. B. einen Schlüssel über „*Drag & Drop*“ in eine andere Gruppe ziehen) muss bestätigt werden. Schlüssel werden immer kopiert oder referenziert. Die Funktion „Ausschneiden“ ist nicht möglich.

- **Schlüsselreferenz aus Gruppe entfernen bestätigen**

  Das Entfernen einer Schlüsselreferenz aus einer Gruppe muss bestätigt werden.

Welcher Security Officer ist angemeldet?

Darüber hinaus wird in diesem Dialog der angemeldete Security Officer angezeigt. Diese Information können Sie ebenfalls aus der Statuszeile der *u.trust LAN Crypt* Admin-Konsole entnehmen.

3.4.2 Benutzereinstellungen

Über den Reiter **Benutzereinstellungen** können Sie die Darstellung von Informationen in der *u.trust LAN Crypt* Administration beeinflussen.

Aktivieren Sie

- *Name der Domäne zum Gruppennamen hinzufügen*, um in der *u.trust LAN Crypt* Administration die Zuordnung zwischen *u.trust LAN Crypt* Gruppen und Domänen dargestellt zu bekommen. Diese Option ist insbesondere dann hilfreich, wenn *u.trust LAN Crypt* bei mehreren Domänen zum Einsatz kommt.

- *Ausgewählte Benutzer und Zertifikate anzeigen*, um sich unter dem Knoten **Zentrale Einstellungen** in *u.trust LAN Crypt* alle importierten Benutzer und deren Zertifikate anzeigen zu lassen.

  Hinweis: Beachten Sie, dass das Anzeigen aller Benutzer und Zertifikate bei größeren Installationen einen Zeitraum von mehreren Minuten in Anspruch nehmen kann. Damit Änderungen an der Option *Ausgewählte Benutzer und Zertifikate anzeigen* wirksam werden, müssen Sie die *u.trust LAN Crypt* Admin-Konsole neu starten.

  Hinweis: Beachten Sie bitte auch, dass bei einem Upgrade oder einer Neuinstallation der u.trust *LAN Crypt* Administration die Option „*Ausgewählte Benutzer und Zertifikate anzeigen*“ ggf. erneut aktiviert werden muss.

- *Elternelemente der Benutzer anzeigen* bedeutet, dass bei den Benutzern auch übergeordnete Objekte angezeigt werden. Unter dem Knoten *Mitglieder und Zertifikate für Gruppe* wird dann auch die Parent-Gruppe des jeweiligen Benutzers angezeigt. Damit können Sie auf einen Blick erkennen, ob die *u.trust LAN Crypt* Datenbank Benutzer enthält, die (noch) keiner Gruppe zugeordnet sind. Damit Änderungen dieser Einstellung wirksam werden, müssen Sie die *u.trust LAN Crypt* Admin-Konsole neu starten.

- *Zwischenspeichern von Benutzerlisten deaktivieren*

  Zur Perfomance-Steigerung baut *u.trust LAN Crypt* standardmäßig Benutzerlisten im Hintergrund auf und setzt den Aufbau auch fort, wenn der Security Officer zu anderen Knoten in der Administration wechselt. Die Ergebnisse des Listenaufbaus werden zwischengespeichert, sodass ein erneuter Abruf dieser Liste keinen Datenbankzugriff erfordert. Dies ist bei umfangreichen Listen sehr zeitsparend.

  Dies führt unter Umständen in Umgebungen mit mehreren parallelen *u.trust LAN Crypt* Administratoren (Terminal Server) zu einem erhöhten Speicherverbrauch. Um das zu verhindern, kann diese Option aktiviert werden. Dadurch werden die Listen nicht zwischengespeichert und der Listenaufbau wird beim Verlassen des Knotens abgebrochen. Es wird empfohlen, diese Option nur dann zu aktivieren, wenn tatsächlich Probleme mit Speicherknappheit auftreten.

  Innerhalb einer Sitzung werden Änderungen in der Datenbank nicht automatisch in eine aufgebaute Liste übernommen.

  Eine Aktualisierung kann jederzeit durch Drücken der Taste *F5* vorgenommen werden.

Hinweis: Änderungen an den oben genannten Einstellungen werden nicht in der Datenbank hinterlegt. Dies sind persönliche Einstellungen, deren Speicherung für jeden Benutzer individuell im Snap-In der Microsoft Management Konsole erfolgt.

3.5 Zentrale Einstellungen

Für den Knoten **Zentrale Einstellungen** können Sie verschiedene Eigenschaften für die *u.trust LAN Crypt* Administration zentral festlegen.

Klicken Sie dazu auf *Eigenschaften* im Kontextmenü des Knotens **Zentrale Einstellungen**. Alternativ können Sie auch das Symbol 'Eigenschaften' in der *u.trust LAN Crypt*-Administrationssymbolleiste anklicken. Sie können die Eigenschaften anschließend über mehrere Reiter einsehen und diese bei Bedarf anpassen.

Hinweis: Die Reiter **Zusätzliche Autorisierung**, **Wiederherstellungsschlüssel** und **Regionen** sind nur für Master Security Officer sichtbar. Die Reiter **Server** und **Konfiguration** sind nur sichtbar und der Reiter **Verzeichnisse** bearbeitbar, wenn der Security Officer das globale Recht *Konfiguration ändern* besitzt. Die Reiter **Algorithmen** und **Zertifikate** sind ausschließlich für den Master Security Officer bearbeitbar. Nur Master Security Officer können Änderungen in den Reitern **Algorithmen**, **Zertifikate** und **Regeln auflösen** vornehmen.

3.5.1 Algorithmen

u.trust LAN Crypt bietet folgende Verschlüsselungsalgorithmen an:

- **AES-128**
- **AES-256**
- **3DES** (nicht mehr sicher)
- **DES** (nicht mehr sicher)
- **IDEA** (nicht mehr sicher)
- **XOR** (nicht mehr sicher)

Wählen Sie aus, welche Algorithmen Sie verwenden wollen. Die hier ausgewählten Algorithmen stehen Ihnen später beim Erzeugen der verschiedenen Schlüssel zur Verfügung.

Hinweis: Werden diese Einstellungen später geändert (z. B. 3DES wird aus der Liste der verfügbaren Algorithmen gestrichen), sind bereits erzeugte Schlüssel und damit verschlüsselte Dateien davon nicht betroffen. Die abgewählten Algorithmen stehen dann nur nicht mehr bei der Erzeugung neuer Schlüssel zur Verfügung. Bei einer Auswahl von Algorithmen, die als nicht mehr sicher gelten, erhalten Sie einen entsprechenden Sicherheitshinweis. Sie können diese Algorithmen aber dennoch weiterhin wählen und verwenden.

Standard Algorithmus

Wählen Sie hier aus, welcher Algorithmus für die automatische Erzeugung von Benutzer -und Gruppenschlüsseln verwendet werden soll. Als Standard-Algorithmus wird **AES** entweder mit **256** oder alternativ mit **128 Bit Schlüssellänge** empfohlen, da sie die höchste Sicherheit bieten.

3.5.2 Schlüssel

Bei der Zusammenführung mehrerer *u.trust LAN Crypt*-Installationen z. B. im Rahmen von Firmenverschmelzungen oder Abteilungszusammenlegungen kann es zu Problemen mit doppelten internen Schlüsselnamen kommen.

Aus diesem Grund werden Schlüssel über eindeutige **G**lobal **U**nique **ID**s (GUID) identifiziert. Die GUID wird standardmäßig von *u.trust LAN Crypt* nach einem Zufallsprinzip generiert und lässt sich nachträglich nicht ändern.

Falls jedoch zwischen zwei Unternehmen ein Austausch von Dateien stattfinden soll, die per *u.trust LAN Crypt* verschlüsselt wurden, wird eine Möglichkeit benötigt, einen gemeinsamen Schlüssel zu erzeugen.

Nur so ist sicherzustellen, dass eine Datei, die von Unternehmen „A“ mit dem Beispielschlüssel `CRYPTOKEY` verschlüsselt wurde, auch von Unternehmen „B“ entschlüsselt werden kann. Voraussetzung hierfür ist, dass Unternehmen „B“ ebenfalls einen Schlüssel namens `CRYPTOKEY` erzeugt, der über dieselben Einstellungen verfügt, wie der Schlüssel von Unternehmen „A“. Dies betrifft auch die GUID des Schlüssels und den Verschlüsselungsalgorithmus.

Für einen solchen Fall bietet *u.trust LAN Crypt* die Möglichkeit, bei der Erzeugung eines neuen Schlüssels die GUID manuell einzugeben. Hierfür muss die Option **Security Officers dürfen die GUID neuer Schlüssel festlegen** aktiviert werden.

Hinweis: Weitere Möglichkeiten zur gemeinsamen Schlüsselverwendung bestehen auch über *LC2Go* (siehe Abschnitt 3.15.1 „*Lc2Go Schlüsselimport*“ auf Seite 133) oder über die *u.trust LAN Crypt API* mithilfe der neuen Funktion *Multi-Policy-Support*.

Hinweis: Diese Einstellung kann nur von einem Master Security Officer geändert werden.

Schlüsselwert

Durch Aktivieren der Option **Nur Security Officer mit dem Recht 'Profile erzeugen' dürfen Schlüssel erzeugen (Schlüssel ohne Wert nicht zulassen)** können Sie sicherstellen, dass nur Security Officer, die die globalen Rechte *Schlüssel erzeugen* und *Profile erzeugen* besitzen, Schlüssel (Namen und Wert) erzeugen können. Wird dem Schlüssel vom Security Officer beim Anlegen kein Wert zugewiesen, dann wird der Wert jedoch beim Speichern des Schlüssels automatisch generiert.

Ist diese Option aktiviert (Standardeinstellung bei einer Neuinstallation), können Security Officer, die das globale Recht *Profile erzeugen* nicht besitzen, keine Schlüssel mehr anlegen.

Die Verwendung von Gruppenschlüsseln (<GROUPKEY>) in Verschlüsselungsregeln ist für diese Security Officer dann ebenfalls nicht mehr möglich.

Hinweis: Wenn ein Security Officer nur Schlüssel, aber keine Profile erzeugen soll, können Sie dies in den Berechtigungen der jeweiligen Gruppen konfigurieren (vgl. Kapitel 3.11.3 „*Dem Security Officer Rechte zur Bearbeitung der Gruppen zuweisen*“ ab Seite 121.

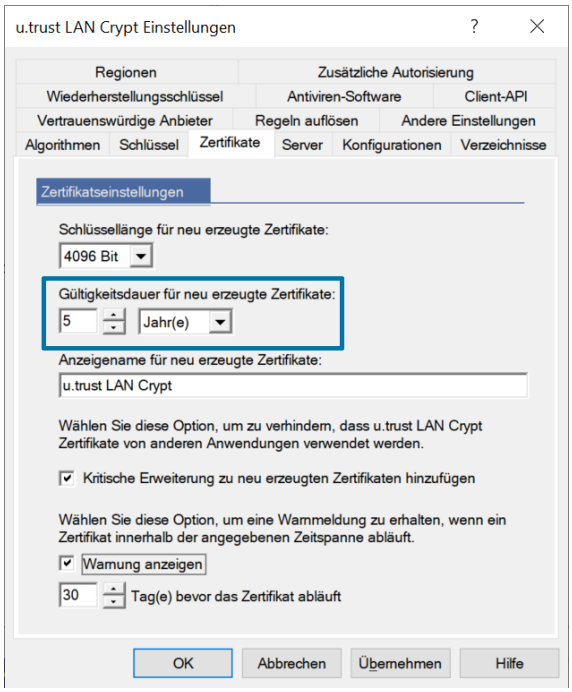
Für Gruppenschlüssel, deren Werte erst beim Erzeugen der Profildateien generiert werden, werden die Werte ebenfalls sofort erzeugt, wenn sie beim Anlegen einer Verschlüsselungsregel verwendet werden.

Hinweis: Die Option **Nur Security Officer mit dem Recht 'Profile erzeugen' dürfen Schlüssel erzeugen (Schlüssel ohne Wert nicht zulassen)** beeinflusst die Verwendung von benutzerspezifischen Schlüsseln (<USERKEY>) in Verschlüsselungsregeln nicht!

Hinweis: Grundsätzlich bietet *u.trust LAN Crypt* auch die Möglichkeit, Schlüssel ohne Wert anzulegen. Mit solchen Schlüsseln kann in der Administration zwar uneingeschränkt gearbeitet werden. Bei verteilten Datenbanken kann dies jedoch zu Problemen führen. Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, wenn in einem Replikationszeitfenster an verschiedenen Standorten Profildateien erzeugt werden, die Schlüssel ohne Wert enthalten (manuelle angelegte Schlüssel ohne Wert, Gruppenschlüssel <GROUPKEY>). Beim Erzeugen der Profildateien würde an jedem Standort folglich ein eigener Wert für den Schlüssel erzeugt. Das Ergebnis wäre ein Schlüssel mit zwei unterschiedlichen Werten.

3.5.3 Zertifikate

Auf dieser Seite können Sie Schlüssellänge für neu erzeugte Zertifikate (1024, 2048, 4096 Bit) und die Gültigkeitsdauer für die von *u.trust LAN Crypt* erzeugten Zertifikate festlegen. Für die von *u.trust LAN Crypt* erzeugten Zertifikate ist eine Gültigkeitsdauer von 1 Jahr vordefiniert. Sie können diesen Wert jederzeit ändern.



Hinweis: Die *Gültigkeitsdauer für neu erzeugte Zertifikate* können Sie zwischen *1 Tag* und maximal *999 Jahren* einstellen. Im Sinne der Informationssicherheit sollte jedoch die Gültigkeitsdauer einen Zeitraum von 5 Jahren nach Möglichkeit nicht überschreiten. Für CA-Zertifikate (**C**ertificate **A**uthority) empfiehlt Utimaco dagegen eine maximale Gültigkeitsdauer von 20 Jahren.

Hinweis: Für Zertifikate, die (Master) Security Officer zugewiesen werden, darf die Gültigkeitsdauer **nicht über das Jahr 3100** hinausgehen.

Unter Anzeigename für neu erzeugte Zertifikate können Sie einen Namen für von *u.trust LAN Crypt* erstellte Zertifikate angeben. Alle Zertifikate erhalten diesen Anzeigenamen und können daher leicht als *u.trust LAN Crypt*-Zertifikate identifiziert werden.

Wenn Sie die Option **Kritische Erweiterung zu neu erzeugten Zertifikaten hinzufügen** wählen, wird zu neu erzeugten Zertifikaten eine kritische Erweiterung hinzugefügt, die anderen Anwendungen zeigt, dass Sie diese Zertifikate nicht verwenden dürfen.

Sie können eine Frist in Tagen bestimmen, innerhalb der eine Warnung (beim Auflösen der Regeln, oder als gelbe Markierung in der Liste der Zertifikate) ausgegeben wird, dass das Zertifikat ablaufen wird. Tragen Sie hier beispielsweise 30 Tage ein, wird ca. ein Monat vor Ablauf des Zertifikats eine Warnmeldung angezeigt, dass das Zertifikat bald nicht mehr gültig sein wird und zu erneuern ist.

3.5.4 Regeln auflösen

Benutzer ohne Zertifikat immer überspringen

Aktivieren Sie diese Option, wenn Benutzer, denen bisher noch kein Zertifikat zugewiesen wurde, beim Erzeugen der Profildateien übersprungen werden sollen. Für solche Benutzer wird dann keine Profildatei erzeugt.

Hinweis: Wird ein Benutzer hinzugefügt, wenn diese Option aktiviert ist und dem Benutzer wurde noch kein Zertifikat zugewiesen, erfolgt keine Warnung, wenn für diesen Benutzer beim Auflösen der Verschlüsselungsregeln keine Profildatei angelegt werden konnte.

Wählen Sie aus, wie die Regeln auf dem Client ausgeführt werden sollen:

Hinweis: Diese Einstellung kommt nur bei Clients ab Version 3.90 zur Anwendung.

Hier können Sie aus drei verschiedenen Sortiermethoden wählen. *Sortiermethode 3* ist die Standardmethode, die von Clients vor Version 3.90 von LAN Crypt verwendet wurde. Bei früheren Versionen konnte die Sortiermethode in LAN Crypt nicht geändert werden.

- **Sortiermethode 1**
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Verschlüsselungsregeln
- **Sortiermethode 2**
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Als absolute Pfade definierte Verschlüsselungsregeln ohne Platzhalter
  4. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, ohne Unterordner

5. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, mit Unterordnern
6. Alle anderen Verschlüsselungsregeln

Ein absoluter Pfad wird entweder als UNC-Pfad (mit doppeltem Backslash zu Beginn) oder als <*Laufwerksbuchstabe*>*:*\ angegeben.

Beispiele für die Anwendung einer Referenz auf einen Schlüssel:

`\\server\share\*.*` oder

`c:\geheim\*.*`

- **Sortiermethode 3 (Standard)**

  Die Sortiermethode 3 unterscheidet nicht zwischen Ignorieren-Regeln, Ausschließen-Regeln und Verschlüsselungsregeln.

  Die Regeln werden in der folgenden Reihenfolge sortiert:

  1. Alle absoluten Pfade ohne Platzhalter
  2. Alle absoluten Pfade mit Platzhaltern, ohne Unterordner
  3. Alle absoluten Pfade mit Platzhaltern, mit Unterordnern
  4. Alle anderen Regeln

  Ein absoluter Pfad wird entweder als UNC-Pfad (mit doppeltem Backslash zu Beginn) oder als <*Laufwerksbuchstabe*>*:*\ angegeben.

  Innerhalb der oben angegebenen Abschnitte (zum Beispiel: *Sortiermethode 3 - Alle anderen Regeln*), richtet sich die Sortierung danach, wie präzise die Pfaddefinition ist.

  Hierbei gilt folgende Reihenfolge:

  1. UNC-Pfade.
  2. Pfade, die mit <*Laufwerkbuchstabe*> beginnen: Hier wird der Backslash nach dem Laufwerksbuchstaben nicht berücksichtigt.
  3. Alle anderen Pfade.

     Zudem gilt:

     - Pfade mit mehr Backslashs werden vor Pfaden mit weniger Backslashs aufgelistet
     - Pfade ohne Platzhalter werden vor Pfaden mit den Platzhaltern ***.** und ***.*** aufgelistet

Hinweis: Änderungen an dieser Option werden auf den Clients wirksam, nachdem neue Profile generiert und verteilt wurden.

Wählen Sie aus, welches Verschlüsselungsformat vom *u.trust LAN Crypt* Client verwendet werden soll

Hier können Sie den Modus konfigurieren, den die Clients bei Einsatz des Verschlüsselungsalgorithmus AES verwenden sollen. *u.trust LAN Crypt* unterstützt folgende Verschlüsselungsmodi:

- CBC-Format (Versionen 3.50 oder höher)

  Dieses Format wird von *LAN Crypt* Clients ab Version 3.50 oder höher verwendet. Diese Clients können Dateien lesen, die im OFB-Modus (Format von Vorgängerversionen) verschlüsselt sind. Für neue Dateien wird der Verschlüsselungsmodus CBC verwendet.

- XTS-AES-Format (Versionen 3.90 oder höher)

  Dieses Format kann von *LAN Crypt* Clients ab Version 3.90 oder höher verwendet werden. Diese Clients können Dateien lesen, die im OFB- und im CBC-Modus verschlüsselt sind. Für neue Dateien wird der Verschlüsselungsmodus XTS-AES verwendet. Dieser Modus wird nur für AES-Schlüssel verwendet. Für andere Blockchiffren als AES wird generell der CBC-Modus verwendet.

- CBC-uIV-Format (Versionen 13.0.0 oder höher)

  Dieses Format kann von *LAN Crypt* Clients ab Version 13.0.0 oder höher verwendet werden. Diese Clients können Dateien lesen, die im OFB-, CBC- und XTS-AES-Modus verschlüsselt sind. Für neue Dateien wird der Verschlüsselungsmodus CBC-uIV verwendet. Um die Sicherheit von CBC zu erhöhen, wird im uIV-Format (**u**npredictable **I**nitialization **V**ector) ein zufälliger und somit nicht vorhersehbarer Initialisierungsvektor verwendet.

  Hinweis: Welche Dateien bereits mit dem neuen *CBC-uIV-Format* verschlüsselt sind, können Sie mithilfe des Kommandozeilen-Tools `encstatus.exe` ermitteln. Sie finden das Kommandozeilen-Tool im Installations-Verzeichnis Ihres extrahierten *u.trust LAN Crypt* Admin Installationspakets.

  Sie können mit `encstatus.exe` den Verschlüsselungsmodus über die Kommandozeile wie folgt prüfen:

  Beispiel: Wenn Sie beispielsweise prüfen wollen, ob und welche Dateien im Ordner „`HR`“ auf dem lokalen Laufwerk „`C:`“ bereits mit dem neuen *CBC-uIV-Format* verschlüsselt sind, öffnen Sie die Kommandozeile auf Ihrem Computer, wechseln Sie in den Ordner, in dem sich das Kommandozeilen-Tool `encstatus.exe` befindet und geben Sie dort den folgenden Befehl ein:

  ```
  ENCSTATUS C:\HR /CNM /DCP /XM CBC-uIV /XM CBC /F /S
  ```

  Hinweis: Eine Beschreibung der jeweiligen Parameter von `encstatus.exe` erhalten Sie, wenn Sie auf der Kommandozeile `encstatus -h` eingeben.

  Hinweis: Beachten Sie außerdem, dass ältere *LAN Crypt* Client-Versionen das CBC-uIV-Format nicht unterstützen! Bevor Sie Dateien in das neue CBC-uIV-Format verschlüsseln, **müssen unbedingt zuerst alle älteren *LAN Crypt* Clients auf die aktuelle Version aktualisiert werden**. Die aktuellen Versionen von *LAN Crypt* für macOS, IOS und Android unterstützen ebenfalls das neue CBC-uIV-Format.

Für Client-Versionen vor Version 3.90 ist nur die folgende Konfiguration gültig:

CBC-Format zur Verschlüsselung mit optionaler Anwendung des Formats von Vorgängerversionen als „altes Verschlüsselungsformat“. Alle anderen Einstellungen werden von diesen Clients ignoriert. Sie verwenden standardmäßig das CBC- oder das Format von Vorgängerversionen.

Dieses Verschlüsselungsformat bis zu folgendem Datum verwenden

Während eines Upgrade-Vorgangs kann ein alter Verschlüsselungsmodus konfiguriert werden. Dieser alte Verschlüsselungsmodus bleibt bis zu einem angegebenen Datum aktiv. Ab diesem Datum müssen alle Clients migriert werden, damit sie den konfigurierten neueren Verschlüsselungsmodus unterstützen. Andernfalls legen neue Clients zwar verschlüsselte Dateien im konfigurierten Verschlüsselungsmodus an, diese Dateien können jedoch nicht von älteren Clients gelesen werden.

Je nach Einstellung für das zu verwendende Verschlüsselungsformat, können die folgenden Formate hier ausgewählt werden:

- **Format von Vorgängerversionen (Versionen 2.x, 3.x)**
- **CBC-Format (Versionen 3.50 oder höher)** ist nur verfügbar, wenn XTS-AES als Verschlüsselungsformat konfiguriert ist. Für CBC ist eine *LAN Crypt* Client-Version ab Version 3.50 oder höher erforderlich.
- **XTS-AES-Format (Versionen 3.90 oder höher)** ist nur verfügbar, wenn CBC-uIV als Verschlüsselungsformat konfiguriert ist. Für XTS-AES ist eine *LAN Crypt* Client-Version ab Version 3.90 oder höher erforderlich. Dieser Modus wird nur für AES-Schlüssel verwendet.

  Ältere *LAN Crypt* Clients werten die Einstellung **Dieses Verschlüsselungsformat bis zu folgendem Datum verwenden** nur dann aus, wenn die Einstellung **Format von Vorgängerversionen** ausgewählt ist.

  Sie müssen festlegen, bis zu welchem Datum die verschlüsselten Dateien weiterhin im alten Format geschrieben werden dürfen. Wird dieses Datum überschritten oder die Option deaktiviert, werden die Dateien im neuen Format geschrieben. Änderungen an dieser Option werden auf den Clients erst nach dem Erzeugen und Verteilen neuer Profile wirksam.

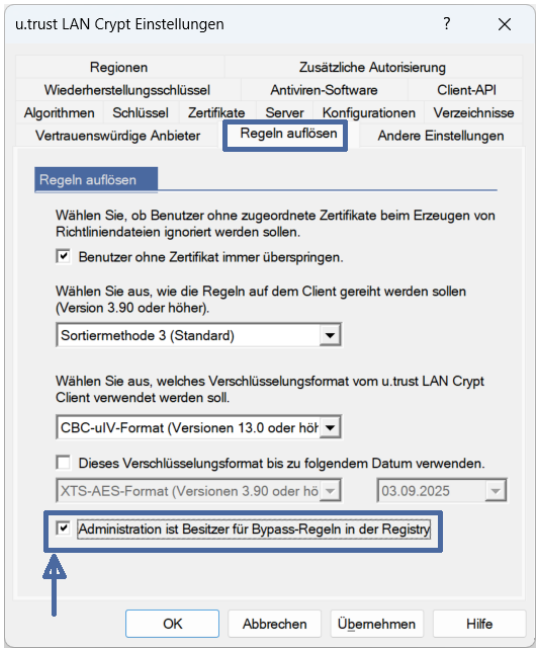
  Nach der Aktualisierung aller Clients empfehlen wir, eine Initialverschlüsselung mit dem *u.trust LAN Crypt* Initialverschlüsselungs-Tool durchzuführen. Damit stellen Sie sicher, dass nur das neue Verschlüsselungsformat verwendet wird.

  Diese Änderungen werden beim nächsten Auflösen der Verschlüsselungsregeln wirksam.

  Hinweis: Bitte beachten Sie, dass verschlüsselte Dateien, die mit dem veralteten Verschlüsselungsmodus OFB erstellt wurden, von *LAN Crypt* ab Version 4.0.0 nur noch gelesen werden können! Beim Schreiben bzw. neu speichern wird der jeweils eingestellte neuere Modus verwendet. Utimaco empfiehlt grundsätzlich alle Dateien, die noch mit dem veralteten Verschlüsselungsmodus OFB verschlüsselt sind, mithilfe der Initialverschlüsselung nach (AES) XTS umzuschlüsseln.

Administration ist Besitzer für Bypass-Regeln in der Registry

Bypass-Regeln dienen dazu, in speziellen Szenarien essenzielle *u.trust LAN Crypt* Funktionen abzuschalten. Das Aktivieren der Bypass-Funktion wirkt sich auf alle Clients aus. *Bypass-Regeln* können Sie über die *u.trust LAN Crypt* Administration (siehe „Bypass-Regel setzen“ auf Seite 152) nur dann erstellen, wenn die Option **Administration ist Besitzer für Bypass-Regeln in der Registry** aktiviert ist.



Warnung: Beachten Sie, dass hierbei äußerste Vorsicht geboten ist! Fehlerhafte Einstellungen könnten u. a. dazu führen, dass Dateien beschädigt (korrumpiert) werden. Deshalb ist das Einführen solcher Regeln kritisch und sollte ausschließlich abgestimmt mit dem Utimaco-Support erfolgen.

Hinweis: Diese Einstellung kann nur von einem Master Security Officer geändert werden.

Beachten Sie: Wenn bereits auf anderem Wege per Gruppenrichtlinie oder Registry *Bypass-Regeln* gesetzt waren, werden diese durch diese neue Funktion überschrieben oder gelöscht.

Hinweis: Um Konflikte mit anderen Regeln zu vermeiden, kann diese Funktion erst dann deaktiviert werden, nachdem alle *Bypass-Regeln* gelöscht wurden.

3.5.5 Server

Zum Importieren der Gruppen und Benutzer von einem Server, benötigt *u.trust LAN Crypt* die Anmeldeinformationen für diesen Server. Diese Informationen müssen im Reiter **Server** angegeben werden. Klicken auf **Hinzufügen** öffnet einen weiteren Dialog mit drei Reitern: *Details*, *Einstellungen* und *Zertifikate*

Server-Details: Anmeldung mit Passwort

1. Geben Sie *Domänen- oder Servername*, *Benutzername* und das dazugehörige *Passwort* ein. Geben Sie bitte zur Vermeidung doppelter Einträge auch einen alternativen Namen als *Alias* für den Server an, falls der Server durch mehrere Namen angesprochen werden kann. Bei Eingabe mehrerer Aliasnamen sind diese jeweils durch ein Semikolon voneinander zu trennen.

   Wenn Sie einen **Microsoft-Verzeichnisdienst** verwenden, gehen Sie wie folgt vor:

   - Geben Sie den Domänennamen unter *Domänen- oder Servername* ein.
   - Geben Sie den *Benutzernamen* als Benutzername@Domäne an.

     Hinweis: Der Benutzername muss in LDAP-Syntax (kanonischer Name) angegeben werden, um Objekte aus einem Verzeichnisdienst, der **nicht** von Microsoft stammt, zu importieren. Beispiel: cn=admin,ou=techops

2. Geben Sie die zu benutzende API an.

   Wählen Sie <*Microsoft*> oder <*Novell*> aus der Dropdown-Liste. Der Platzhalter <*Novell*> steht für alle Nicht-Microsoft-APIs.

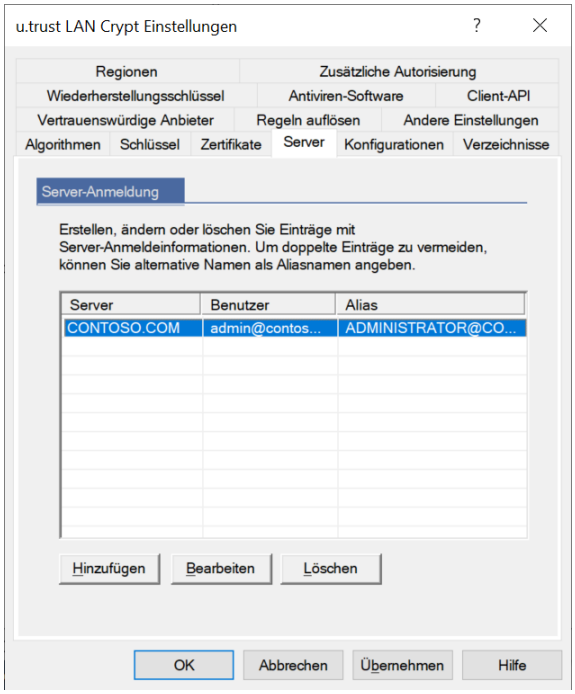
   Hinweis: Der Import aus einem Novell-Verzeichnisdienst wird seit *LAN Crypt* Version 3.90 nicht mehr unterstützt. Auch andere Novell-Funktionalitäten werden ebenfalls nicht mehr unterstützt und sind in der Administration nicht funktionsfähig.

3. Geben Sie die LDAP-Authentisierungsmethode an, die für den Zugriff auf den Server benutzt werden soll, wenn dieser über ein Passwort erfolgen soll. *u.trust LAN Crypt* bietet folgende Methoden:

   - Passwort (LDAP)
   - Passwort (LDAP mit SSL)

4. Klicken Sie auf **OK**.

Der Server wird in der Tabelle *Server-Anmeldung* auf dem Reiter *Server* angezeigt.



Fehlermeldung beim Fehlschlagen der Anmeldung

Wenn *u.trust LAN Crypt* die Anmeldung an dem Server nicht durchführen kann, wird eine Fehlermeldung in der *u.trust LAN Crypt* Administration angezeigt.

Server Details: Anonyme Anmeldung

1. Geben Sie den *Servernamen* ein. Geben Sie bitte zur Vermeidung doppelter Einträge auch einen alternativen Namen als *Alias* für den Server an, falls der Server durch mehrere Namen angesprochen werden kann.

2. Geben Sie die zu benutzende API an.

   Wählen Sie <*Microsoft*> oder <*Novell*> aus der Dropdown-Liste. Der Platzhalter <*Novell*> steht stellvertretend für alle Nicht-Microsoft-APIs.

   Hinweis: Der Import aus einem Novell-Verzeichnisdienst wird seit *LAN Crypt* Version 3.90 nicht mehr unterstützt. Auch andere Novell-Funktionalitäten werden ebenfalls nicht mehr unterstützt und sind in der Administration nicht funktionsfähig.

3. Geben Sie die LDAP-Authentisierungsmethode an, die für den Zugriff auf den Server benutzt werden soll. *u.trust LAN Crypt* bietet folgende Methoden für die anonyme Anmeldung:

   - Anonym (LDAP)
   - Anonym (LDAP mit SSL)

4. Klicken Sie auf **OK**.

Der Server wird in der Tabelle *Server-Anmeldung* unterhalb der Spaltenüberschrift *Server* angezeigt.

Fehlermeldung beim Fehlschlagen der Anmeldung

Wenn *u.trust LAN Crypt* die Anmeldung an den Server nicht durchführen kann, wird eine Fehlermeldung in der *u.trust LAN Crypt* Administration angezeigt.

Einstellungen

Identifizierung der Objekte

u.trust LAN Crypt identifiziert importierte Objekte im Active Directory (AD) anhand einer eindeutigen, immer gleichbleibenden GUID (**G**lobal **U**nique **ID**). Diese GUID wird auch bei der Synchronisation von Datenbank und Verzeichnisdienst verwendet, da z. B. die Namen der einzelnen Objekte sich ändern können, um sicherzustellen, dass Änderungen im AD auch in die Datenbank übernommen werden und nicht aufgrund des neuen Namens in der Datenbank ein neues Objekt erzeugt wird.

Einige andere Verzeichnisdienste verwenden diesen ID-Typ jedoch nicht. In diesem Fall stellt *u.trust LAN Crypt* eine andere Methode zur eindeutigen Identifizierung von Objekten zur Verfügung. *u.trust LAN Crypt* kann so konfiguriert werden, dass bestimmte LDAP-Attribute zur eindeutigen Identifizierung der Objekte verwendet werden. Die jeweils zu verwendenden Attribute können in der *u.trust LAN Crypt* Administration frei konfiguriert werden.

Die Einstellungen <*Standard*> und <*Andere*> stehen immer zur Verfügung. Im Normalfall wird die Einstellung <*Standard*> für den Server, auf den sich die Einstellung bezieht, ausreichen. Unter <Standard> werden jeweils die Attribute angezeigt, die bei Einstellung <Standard> ausgewertet werden. Einerseits wird dadurch angezeigt, welche Attribute in der Standardeinstellung ausgewertet werden. Andererseits können Sie ein spezifisches Attribut angeben, sofern dieses Attribut im betroffenen Verzeichnisdienst existiert. Über <Andere> können andere, als die zur Auswahl stehenden Attribute angegeben werden.

Achtung: Wenn Sie hier ein Attribut angeben, müssen Sie sicherstellen, dass dieses Attribut auch Daten enthält, die eine eindeutige Identifizierung ermöglichen.

- **Objekt-GUID**

  Hier können Sie einstellen, welches Attribut zur Identifizierung verwendet wird. Belassen Sie die Einstellung auf <Standard>, so werden beide Attribute GUID und objectGUID ausgewertet.

  Wenn Sie ein anderes LDAP-Attribut zur Identifizierung der Objekte verwenden wollen, wählen Sie <*Andere*> als *Objekt-GUID* und geben Sie in das rechte Eingabefeld den Namen des LDAP-Attributs an. Dieses Attribut muss Daten enthalten, die eine eindeutige Identifizierung des Objekts erlauben.

- **GUID-Attribut ist ein binärer Wert**

  Diese Option hat nur Auswirkungen für die Darstellung der GUID in den *Eigenschaften* Dialogen der Objekte. Damit diese korrekt dargestellt werden, sollten Sie diese Option

aktivieren, wenn es sich bei der verwendeten GUID um einen binären Wert handelt. Im Zweifelsfall aktivieren Sie bitte diese Option.

Hinweis: Diese Einstellung ist standardmäßig aktiviert. Sie können diese Einstellung nur ändern, wenn Sie *<Andere>* als *Objekt-GUID* gewählt haben.

Attribute für Benutzer

- **Attribut für Benutzername**

  Diese Einstellung wirkt sich nur auf die Anzeige der Benutzer in der *u.trust LAN Crypt* Administration aus. Die Benutzer werden im Dialog *Eigenschaften einer Gruppe* und im SnapIn *Benutzer und Zertifikate* angezeigt.

  Sie können eines der vorgegebenen Attribute auswählen oder durch Auswahl von <Andere> ein LDAP-Attribut angeben. <Standard> wertet (CN und SN) aus.

- **Attribut für Anmeldename**

  Dem Attribut für den *Anmeldenamen* kommt eine besondere Bedeutung zu. *u.trust LAN Crypt* benennt die Profildateien nach dem *Anmeldenamen* der Benutzer. Nur wenn der *Anmeldename* und der Name der Profildatei identisch sind, kann sich der Benutzer beim *u.trust LAN Crypt* Client anmelden.

  Hier können Sie bestimmen durch welches LDAP-Attribut der *Anmeldename* des Benutzers festgelegt wird.

  <Standard> wertet *SAMAccountName*, *userPrincipalName* und *UID* aus. Sollten zwei oder drei dieser Attribute im Verzeichnisdienst existieren, können Sie hiervon eines auswählen, das den *Anmeldenamen* des Benutzers bestimmt.

  <Andere> ermöglicht die Angabe eines weiteren Attributs, das im Verzeichnisdienst den *Anmeldenamen* enthält.

  Hinweis: Sollte der Name im Attribut das @-Zeichen enthalten, trennt *u.trust LAN Crypt* jedoch den Namen an dieser Stelle ab. Dies kann z. B. bei der Verwendung von E-Mail-Adressen als Anmeldename zu Problemen führen.

- **Attribut für E-Mail-Adresse**

  Dieses Attribut wird in selbst erzeugte Zertifikate eingefügt.

- **Attribut für Kommentar**

  Dieses Attribut kann, wie die E-Mail-Adresse zur besseren Identifizierung der Benutzerobjekte verwendet werden. Das ist vor allem dann hilfreich, wenn Benutzername und Anmeldename nicht zur Objektidentifizierung beim Assistenten zur Zertifikatszuordnung geeignet sind. Der Name des Attributs anhand dessen der zugehörige Benutzer vom Assistenten zur Zertifikatszuordnung gefunden werden soll, kann hier eingetragen werden.

Hinweis: Werden bei einer Synchronisierung leere Attribute importiert (wenn z. B. ein Attribut im AD gelöscht wurde), sind die *u.trust LAN Crypt* Kommentare davon nicht betroffen. Die bestehenden Einträge bleiben weiterhin erhalten. Änderungen der Kommentare sind aber weiterhin möglich, wenn z. B. das Attribut durch den Security Officer in *u.trust LAN Crypt* geändert wird.

Bei Auswahl von <Standard> wird kein Kommentar importiert.

- **Zertifikate**

  Wenn Sie den Reiter *Zertifikate* wählen, können Sie dort festlegen, ob Zertifikate, die dem Benutzer über das LDAP-Verzeichnis zugewiesen wurden, beim Importieren der Benutzer in die *u.trust LAN Crypt* Datenbank übernommen und auch zugewiesen werden sollen.

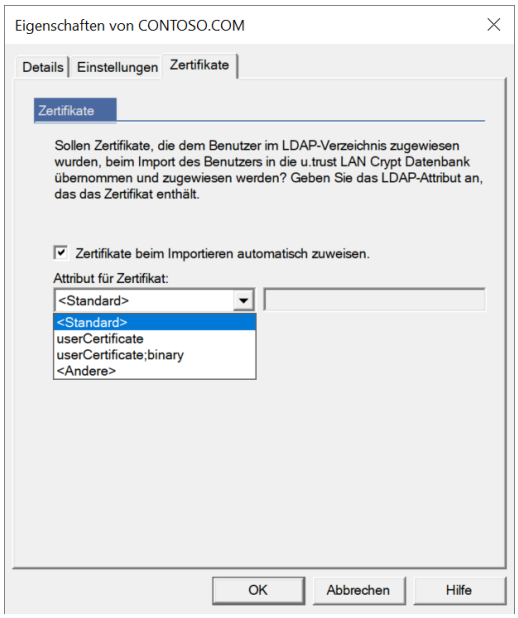
  Eine Zuordnung der Zertifikate über die *u.trust LAN Crypt* Admin-Konsole ist für diese Benutzer dann nicht mehr erforderlich. Sie haben auch hier die Möglichkeit, ein Attribut anzugeben, welches das Zertifikat für den Benutzer enthält.

Hinweis: Zertifikate, die dem Benutzer auf diese Weise zugewiesen wurden, werden von *u.trust LAN Crypt* nicht geprüft (Gültigkeitsdauer, auf einer CRL, usw.)!

Aktivieren Sie die Option

Zertifikate beim Importieren automatisch zuweisen

wenn die Zertifikate aus dem LDAP-Verzeichnis automatisch beim Übernehmen in die *u.trust LAN Crypt* Datenbank importiert und dem Benutzer zugewiesen werden sollen.



Das Attribut <Standard> wertet userCertificate und userCertificate;binary aus.

Klicken Sie auf <Andere>, um ein weiteres Attribut anzugeben, das das Zertifikat enthält.

Durch Klicken auf **OK** werden die Anmeldeinformationen in die Liste der Server übertragen. Dort können diese Angaben auch bearbeitet oder gelöscht werden.

3.5.6 Verzeichnisse

Hinweis: Die hier vorgenommenen Einstellungen werden immer im aktuellen Konfigurationssatz des Security Officers gespeichert. Wurden noch keine Konfigurationssätze erstellt, ist das der Konfigurationssatz <STANDARD KONFIGURATION>.

Hinweis: Beachten Sie, dass im Knoten **Zentrale Einstellungen** im Reiter *Verzeichnisse* für Pfadangaben keine Umgebungsvariablen, wie z. B. `%LOGONSERVER%` etc. verwendet werden können.

Speicherort für erzeugte Richtliniendateien

Sie müssen angeben, an welchem Speicherort bzw. Pfad die für die Benutzer erzeugten Profildateien gespeichert werden sollen.

Geben Sie in das Eingabefeld den Speicherort (in der Regel ein für die Benutzer freigegebenes Netzwerklaufwerk) an.

Hinweis: Bitte achten Sie darauf, dass dieser Pfad für die Benutzer erreichbar ist, da die Clients bei der Anmeldung von dort die Profildateien laden.

Achtung: Bitte vergessen Sie nicht den Speicherort für die Profildateien auch aus Clientsicht einzustellen. Sie stellen dies über die *u.trust LAN Crypt* Konfiguration mithilfe einer für die Benutzer gültigen Gruppenrichtlinie ein (siehe „*Speicherort für Richtliniendatei*“ auf Seite 181).

Optionen für die Richtliniendatei - Dateiformat festlegen

Wenn Sie verschiedene *LAN Crypt* Client-Versionen (z. B. auch frühere Versionen 3, 4 und 11) verwenden, müssen Sie sicherstellen, dass alle Ihre *LAN Crypt* Clients die generierten Profildateien verarbeiten können. Grundsätzlich wird empfohlen, immer nur die aktuelle *u.trust LAN Crypt* Version zu verwenden.

Hinweis: *LAN Crypt* unterstützt ab Version 4.0.0 keine älteren Profildateiformate (wie z. B. „*.pol.bz2*“ oder „*.pol*“) mehr. Das aktuelle Format der Profildateien ist „*.xml.bz2*“. Dieses Format wird von *LAN Crypt* bereits seit Version 3.90 unterstützt. Hierbei handelt es sich um eine komprimierte XML-Datei. Diese enthält alle zugewiesenen Regeln, Zugriffsrechte und Schlüssel des jeweiligen Benutzers sowie die Signatur des Security Officers. Die in der Profildatei enthaltenen Schlüssel sind mit dem Zertifikat des Benutzers verschlüsselt. Sollten Sie ältere Client-Versionen als 3.97 von *LAN Crypt* verwenden, müssen Sie diese zunächst auf Version 3.97, danach auf Version 4.2.0 und im Anschluss auf Version 11.0.x upgraden, bevor Sie Version 13.0.1 installieren. **Bitte beachten Sie auch, dass das Format für die Profildatei vordefiniert ist und ab Version 4.0.0 nicht mehr geändert werden kann.**

Zusätzliche Richtliniendateien basierend auf dem Novell-Namen erzeugen

Wenn Sie diese Option auswählen, generiert *u.trust LAN Crypt* für jeden Benutzer zwei Profildateien: Eine mit dem Novell- und eine mit dem Windows-Anmeldenamen. Inhaltlich sind beide Dateien identisch.

Die Benutzung des Novell-Anmeldenamens muss auch in der *u.trust LAN Crypt*-Gruppenrichtlinie definiert sein, damit dieser ebenfalls zur Anmeldung benutzt werden kann.

Hinweis: Diese Funktion wird von *LAN Crypt* ab Version 4.0.0 nicht mehr unterstützt.

Speicherort für erzeugte Zertifikate und Schlüsseldateien (.p12)

u.trust LAN Crypt kann bei Bedarf selbst-signierte Zertifikate (*.p12*-Schlüsseldateien) erzeugen und diese den Benutzern zuweisen. Diese Zertifikate werden in der *u.trust LAN Crypt* Admin-Konsole über den Knoten **Ausgewählte Benutzer und Zertifikate** angelegt und zugewiesen. Alternativ steht diese Funktion auch über den Knoten **Gruppen**/**Mitglieder und Zertifikate für Gruppe** zur Verfügung.

Hinweis: Sollte der Knoten **Ausgewählte Benutzer und Zertifikate** in der Admin-Konsole nicht angezeigt werden, prüfen Sie unter dem Knoten **u.trust LAN Crypt Administration**, nach Klicken im Kontextmenü auf *Eigenschaften*, ob im Reiter **Benutzereinstellungen** die Option *Ausgewählte „Benutzer und Zertifikate“ anzeigen*, aktiviert ist.

Der Pfad, an welchem Ort diese Dateien gespeichert werden sollen, muss in der *u.trust LAN Crypt* Admin-Konsole im Knoten **Zentrale Einstellungen** auf dem Reiter *Verzeichnisse* angegeben werden. Die Clients bekommen diesen Zugriffspfad entweder über eine Einstellung in der *u.trust LAN Crypt* Gruppenrichtlinie übermittelt („*Speicherort für Schlüsseldatei*“) oder durch einen Eintrag in der Registry, beispielsweise über eine Registry-Datei (*.reg).

Der *u.trust LAN Crypt Client* sucht zuerst im lokalen Zertifikate-Speicher des Computers nach einem passenden Zertifikat, anschließend (falls keines gefunden wurde) in dem per Gruppenrichtlinie oder über die Registry-Einstellung definierten Pfad. Auch der öffentliche Teil des Security Officer Zertifikats (*.cer*), wird von der *u.trust LAN Crypt* Admin-Konsole in diesem Pfad gespeichert (GPO-Einstellung „Speicherort für *Security Officer Zertifikate*“).

Damit die Benutzer-Schlüsseldateien automatisch ihren Inhabern zugewiesen werden können, müssen die Dateinamen den Anmeldenamen der Benutzer (“Anmeldename.p12”) entsprechen.

Wird eine entsprechende Datei gefunden, erscheint ein PIN-Dialog. Diese PIN (enthalten in der Passwortprotokolldatei „*p12pwlog.csv*“), muss dem Benutzer per PIN-Brief oder über einen anderen sicheren Weg mitgeteilt werden, wie z. B. über das im Installationspaket neu enthaltende Tool „*LCSendP12Password*“. Das Zertifikat und der dazugehörige Schlüssel werden nach Eingabe der PIN automatisch importiert.

Wird eine entsprechende „**.cer*“-Datei gefunden, die den öffentlichen Teil des Security Officer Zertifikats enthält, wird diese automatisch importiert.

Alternativ hierzu können die Schlüsseldateien der Benutzer und der öffentliche Teil des Zertifikats des (Master) Security Officers auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide Dateien von den Clients importiert werden können.

Hinweis: Auf den Clients muss immer der öffentliche Teil des Zertifikats jenes Security Officers importiert werden, der die Profildateien erzeugt und signiert hat. Wird der Pfad, unter dem die „*.cer*“-Dateien der Security Officer und die „*.p12*“-Schlüsseldateien der Benutzer gespeichert werden, nach dem Anlegen der Security Officer geändert (beispielsweise durch das Hinzufügen einer Region in Verbindung mit einer Änderung der Pfade in der Konfiguration), müssen die dazugehörigen Zertifikate in den neuen Pfad kopiert werden. Die zuvor verwendeten öffentlichen Zertifikate der Security Officer können andernfalls von den *u.trust LAN Crypt* Clients nicht mehr gefunden werden.

Standardpasswort für Benutzer-Schlüsseldateien

u.trust LAN Crypt bietet darüber hinaus die Möglichkeit, alle Benutzer-Schlüsseldateien mit einem einheitlichen Standardpasswort auszustatten.

Dazu muss eine Datei, die das gewünschte Passwort enthält (maximal 60 Zeichen), in den gleichen Pfad kopiert werden, in dem sich auch die Passwortprotokolldatei befindet (siehe Abschnitt „*Passwortprotokolldatei*“ auf der nächsten Seite).

Die Datei mit dem Standardpasswort muss dabei den gleichen Namen wie die Passwortprotokolldatei (Standardname: p12pwlog.csv) selbst haben, jedoch mit der Dateiendung „*.pwd*“ (analog zum Standardnamen der Passwortprotokolldatei: p12pwlog.pwd). Ist eine solche Datei vorhanden, erhalten alle erzeugten Benutzer-Schlüsseldateien dasselbe Passwort.

Hinweis: Bei Verwendung eines „Standardpasswortes für Benutzer-Schlüsseldateien“ ist unbedingt darauf zu achten, dass sich nicht mehrere „*.p12“*-Schlüsseldateien für ein und denselben Benutzer im Speicherort für erzeugte Zertifikate und Schlüsseldateien (*.p12*) befinden dürfen.

Wird in dieser Datei anstelle des Standardpassworts das Schlüsselwort *logonname* eingetragen, wird der Anmeldename des jeweiligen Benutzers als Passwort verwendet.

Hinweis: Alle „*.p12“*-Schlüsseldateien für (Master) Security Officer erhalten wegen der höheren Sicherheit IMMER ein zufällig generiertes Passwort.

Speicherort für erzeugte Security Officer Zertifikate

u.trust LAN Crypt speichert, z. B. für Backup-Zwecke, Security Officer Zertifikate in *.p12*-Dateien (Schlüsseldateien). Diese Dateien enthalten auch den privaten Schlüssel des Zertifikats. Der Speicherort der Schlüsseldateien für Security Officer ist hier einzutragen.

Hinweis: Da es sich hierbei um sensible Daten handelt, müssen diese unbedingt vor unberechtigtem Zugriff geschützt werden!

Passwortprotokolldatei

Hier können Speicherort und Name für die Passwortprotokolldatei der generierten PKCS#12-Dateien angegeben werden (Standardname: p12pwlog.csv). Diese Datei enthält die Passwörter der erzeugten PKCS#12-Schlüsseldateien und kann z. B. für die Erstellung eines PIN-Briefs verwendet werden.

Die Passwortprotokolldatei enthält folgende Informationen (die Schlüsselwörter in Klammern repräsentieren die jeweiligen Spaltenüberschriften in der „*.csv*“-Datei):

- Datum der Erstellung (CreateDate)
- Uhrzeit der Erstellung (CreateTime)
- Ablaufdatum (ExpirationDate)
- Genaue Uhrzeit, wann die Gültigkeit abläuft (ExpirationTime)
- Benutzername (Name)
- Anmeldename (Logonname)
- E-Mail-Adresse (EMail)
- Erstellungsmodus/-kontext (Mode). Mögliche Werte sind:
  <GUI>-Zertifikat wurde im Dialog *Eigenschaften* des Benutzers erzeugt.
  <SO>-Zertifikat eines SO. Wurde beim Anlegen eines Security Officers erzeugt.
  <WIZARD>-Zertifikat wurde mit dem Assistenten zur Zertifikatszuordnung erzeugt.
- Dateiname (FileName)
- Passwort (Password)

Hinweis: Diese Datei sollte geschützt werden und unter keinen Umständen im gleichen Pfad wie die Profildateien oder Zertifikate gespeichert werden.

Mit *u.trust LAN Crypt* können Sie die Passwortprotokolldatei auf einfache Art und Weise schützen. Installieren Sie hierzu die *u.trust LAN Crypt* Komponenten Admin-Konsole und Clientanwendung auf demselben Computer. Erstellen Sie nach dem Anlegen des initialen Master Security Officers eine Verschlüsselungsregel, mit der die Passwortprotokolldatei verschlüsselt wird. Hierzu erzeugen Sie für den ersten Master Security Officer (MSO) eine Profildatei und laden Sie danach über den *u.trust LAN Crypt* Client diese Profildatei. Der verwendete Verschlüsselungsschlüssel sollte dabei ausschließlich den Master Security Officers und den Security Officers zur Verfügung stehen, die das Recht besitzen, Zertifikate zu erzeugen.

Hinweis: Wenn Sie beide *u.trust LAN Crypt* Komponenten, Admin-Konsole und Clientanwendung auf demselben Computer installieren, **müssen diese unbedingt von der gleichen Version sein**!

Durch Ausführen des Assistenten zur Initialverschlüsselung wird die Passwortprotokolldatei verschlüsselt und kann fortan von unautorisierten Personen nicht mehr eingesehen werden. Um sicherzustellen, dass das Passwort für den initialen Master Security Officer nicht manipuliert wurde, als die Datei noch nicht verschlüsselt war, erstellen Sie ein neues Zertifikat und weisen Sie es dem initialen Master Security Officer zu.

Hinweis: Wenn der Security Officer, der die Zertifikatszuordnung durchführt, im Dateisystem kein Recht hat, die Passwortprotokolldatei zu ändern, können von diesem keine *u.trust LAN Crypt*-Zertifikate erzeugt werden.

Passwortlänge für Schlüsseldateien einstellen

Die Passwortlänge für Schlüsseldateien (.p12-Dateien) beträgt standardmäßig 20 Zeichen. Ab *u.trust LAN Crypt* Version 13.0.0 können Sie in Abhängigkeit Ihrer Sicherheitsanforderungen die Passwortlänge für die von *u.trust LAN Crypt* selbst erzeugten PKCS#12-Dateien (Schlüsseldateien, die das Zertifikat und den privaten Schlüssel enthalten) flexibel zwischen 12 und 60 Zeichen einstellen.

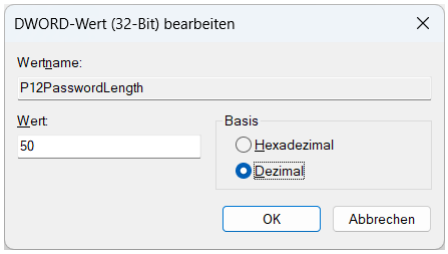
Fügen Sie hierzu den DWORD-Wert mit dem Namen „P12PasswordLength“ in der Windows-Registrierung unter dem Schlüssel

```
[HKLM\SOFTWARE\Policies\Utimaco\SGLANCrypt]
```

hinzu. Tragen Sie dort einen Wert (dezimal) zwischen „12“ und „60“ ein und klicken Sie auf **OK**.

Beispiel:

```
"P12PasswordLength"=dword:0x00000032 (50)
```



Im Beispiel wurde das Passwort auf eine Länge von 50 Zeichen geändert.

Hinweis: Ein Neustart des Rechners ist nach einer Änderung des Wertes nicht erforderlich.

3.5.7 Regionen

u.trust LAN Crypt ermöglicht optional die Angabe von Regionen, um die Administration der Schlüssel übersichtlicher zu gestalten. Die Region wird dem zuständigen Security Officer zugeordnet. Bei der Erzeugung der Schlüssel durch diesen Security Officer wird dem Schlüsselnamen automatisch das Präfix für diese Region vorangestellt. Dadurch ist immer ersichtlich, für welche Administrationseinheit ein Schlüssel erzeugt wurde. Diese Vorgehensweise empfiehlt sich vor allem in verteilten Umgebungen.

Regionen können Sie durch Klicken auf *Eigenschaften* im Kontextmenü des Knotens **Zentrale Einstellungen** im Reiter *Regionen* definieren. Die hier angezeigten Regionen können beim Anlegen der Security Officer diesen zugeordnet werden. Durch Klicken auf **Hinzufügen** können Sie eine neue Region definieren. Geben Sie in das Eingabefeld *Name für die Region* einen treffenden Namen (z. B. Hessen) für die entsprechende Region sowie in das Eingabefeld *Kürzel für die Region* das dazugehörige Präfix für die Region (z. B. HE) ein. Durch Klicken auf die Schaltfläche **OK** wird die neue Region in die Liste der bestehenden Regionen eingetragen.

Bestehende Regionen können bearbeitet und auch gelöscht werden, indem Sie sie markieren und anschließend auf **Bearbeiten** bzw. **Löschen** klicken.

Hinweis: Eine Region kann nur dann gelöscht werden, wenn sie keinem Security Officer zugeordnet ist.

3.5.8 Konfigurationen

Über den Reiter *Konfigurationen* im Knoten **Zentrale Einstellungen** können für die einzelnen Regionen individuelle Konfigurationssätze erstellt werden. Ein so definierter Konfigurationssatz gilt dann nur für die jeweilige Region. Die Administration einzelner Regionen kann über ausgewählte Security Officers erfolgen, wenn Sie diese der jeweiligen Region zuteilen.

Die Konfigurationssätze enthalten die gleichen Angaben, die über den Reiter *Verzeichnisse* eingegeben werden können:

- den Speicherort für erzeugte Profildateien
- den Speicherort für erzeugte Zertifikate und Schlüsseldateien
- den Speicherort für erzeugte Security Officer Zertifikate
- Speicherort und Namen der Passwortprotokolldatei
- die Optionen für die Profildateien

Die Konfigurationssätze werden immer einer bestehenden Region zugeteilt. Für einen einer Region zugeteilten Security Officer steht immer nur der Konfigurationssatz zur Verfügung, der für diese Region erzeugt wurde. Ausgenommen davon ist der Konfigurationssatz <STANDARD KONFIGURATION>, der in jeder Region zur Verfügung steht.

Die Verwendung einer bestimmten Konfiguration für eine Organisationseinheit (die Sie ebenfalls als Region definieren können) stellt sicher, dass die richtigen Pfade für einen oder mehrere Security Officer einfach gesetzt werden können und dass alle Security Officer stets die für ihre Region oder Organisationseinheit definierten Pfade zum Speichern der erzeugten Dateien (z. B. Zertifikate, Profildateien, Passwortprotokolldatei, etc.) verwenden.

Änderungen von Angaben im Reiter *Verzeichnisse* werden immer im aktuell zugewiesenen Konfigurationssatz gespeichert.

Hinweis: Das globale Recht *Konfiguration ändern* steuert, ob ein Security Officer in der Lage sein soll, seine Konfigurationseinstellungen selbst zu ändern. Wird es einem Security Officer nicht gewährt, kann er nur die voreingestellten Pfade der Region verwenden, der er angehört.

Ein Security Officer, der einen bestehenden Konfigurationssatz verändert, ändert damit immer auch die Konfiguration aller Security Officers, denen ebenfalls diese Konfiguration bzw. Region zugewiesen ist!

Konfigurationssatz erzeugen

Zum Erzeugen eines Konfigurationssatzes:

1. Wählen Sie eine bestehende Region aus, für die der Konfigurationssatz erstellt werden soll, oder wählen Sie <Keine Region>, um einen Konfigurationssatz zu erstellen, der Security Officer zugeteilt werden kann. Wählen Sie <Keine Region> nur dann, wenn diese Security Officer keiner Region zugewiesen werden sollen.

2. Geben Sie unter *Neuer Name* eine Bezeichnung für den neuen Konfigurationssatz ein (z. B. München).

3. Markieren Sie einen bestehenden Konfigurationssatz in der Liste.

   Dieser Konfigurationssatz wird kopiert und unter dem neuen Namen gespeichert. Klicken Sie auf die Schaltfläche **Kopieren**.

4. Durch Markieren des Konfigurationssatzes und Klicken auf **Bearbeiten** können Sie diesen editieren.

5. Der angezeigte Dialog entspricht inhaltlich dem des Reiters *Verzeichnisse*. Geben Sie hier die entsprechenden Pfade für die Region ein. Klicken Sie auf **OK**.

6. Der neue Konfigurationssatz wird nun in der Liste unter der entsprechenden Region angezeigt und kann beim Anlegen weiterer Security Officer verwendet werden. Die Konfiguration (und die Region) eines bereits vorhandenen Security Officers kann über die *Eigenschaften* Seite des jeweiligen Security Officers geändert werden.

7. Sie können beliebig weitere Konfigurationssätze anlegen.

3.5.9 Zusätzliche Autorisierung

In *u.trust LAN Crypt* kann festgelegt werden, dass bestimmte Aktionen einer zusätzlichen Autorisierung durch mindestens einen zweiten Security Officer bedürfen. Eine zusätzliche Autorisierung kann für folgende Aktionen verlangt werden:

Aktionen	Notwendige Rechte
Einstellungen für zusätzliche Autorisierung ändern	Darf nur von einem Master Security Officer ausgeführt werden.
Wiederherstellungsschlüssel ändern	Darf nur von einem Master Security Officer ausgeführt werden.

Die folgenden Aktionen dürfen nur von Security Officers ausgeführt werden, die als globales Recht *Operationen autorisieren* und das der Aktion entsprechende Recht besitzen.

Achtung:

Bitte beachten Sie, dass nur der alleinige Besitz eines globalen Rechts zum Ausführen einer zusätzlichen Autorisierung unter Umständen nicht ausreichend sein kann. Die zusätzlichen Security Officers benötigen dieses Recht explizit für das Objekt, an dem die zusätzliche Autorisierung ausgeführt wird.

Aktionen	Notwendige Rechte
Globale Einstellungen ändern	Erfordert das globale Recht *Konfiguration ändern*. Eine Autorisierung wird bei Änderungen in den Reitern **Algorithmen**, **Zertifikat**, **Regionen**, **Verzeichnisse**, **Schlüssel**, **Antiviren-Software**, **Regeln auflösen**, **Server**, **Konfiguration** und **Andere Einstellungen** verlangt. Änderungen in den Reitern **Algorithmen**, **Zertifikate**, **Schlüssel**, **Regeln auflösen**, **Regionen** und **Andere Einstellungen** dürfen nur von einem Master Security Officer autorisiert werden!
Security Officer anlegen	Erfordert das globale Recht *Security Officer erzeugen*.
Zugriffslisten ändern	Erfordert das globale Recht *ACL ändern* und die entsprechenden gruppenspezifischen bzw. Security Officer-spezifischen Rechte.
Globale Rechte ändern	Erfordert das globale Recht *Globale Rechte ändern* und die entsprechenden Security Officer-spezifischen Rechte.
Zertifikate zuweisen	Erfordert das globale Recht *Zertifikate zuweisen* und die entsprechenden gruppenspezifischen bzw. Security Officer-spezifischen Rechte.

Aktionen	Notwendige Rechte
Benutzer- und gruppenspezifische Schlüssel in Regeln verwenden	Erfordert das globale Recht *Spezifische Schlüssel verwenden*. Wenn Sie die zusätzliche Autorisierung für die Verwendung von spezifischen Schlüsseln festlegen, so hat dies keine Auswirkungen auf die Anwendung der Platzhalter <userkey> und <groupkey>. Dies schränkt nur die Handhabung (anzeigen / benutzen / bearbeiten) eines tatsächlichen, spezifischen Schlüssels ein.
Gruppen verwalten	Erfordert das globale Recht *Gruppen ändern* und die entsprechenden gruppenspezifischen Rechte.
Benutzer verwalten	Erfordert das globale Recht *Benutzer ändern* und die entsprechenden gruppenspezifischen Rechte.
Protokollierung verwalten	Erfordert die globalen Rechte *Protokoll lesen* und *Protokollierung verwalten*.
Regeln erzeugen	Erfordert das globale Recht *Regel erzeugen* und das entsprechende gruppenspezifische Recht.
Schlüssel erzeugen oder verschieben	Erfordert das globale Recht *Schlüssel erzeugen* und das entsprechende gruppenspezifische Recht.
Profile erzeugen	Erfordert das globale Recht *Profile erzeugen* und das entsprechende gruppenspezifische Recht.
Schlüsselwert anzeigen	Erfordert das globale Recht *Schlüssel lesen*. Wenn Sie die Option *Schlüsselwert anzeigen* im Eigenschaftendialog eines Schlüssels auswählen, ist eine zusätzliche Autorisierung erforderlich.

Hinweis: Wenn für die Ausführung bestimmter Aktionen eine zusätzliche Autorisierung erforderlich sein soll, gilt diese Einstellung auch für die damit im engen Zusammenhang stehenden Aktionen. Erfordert beispielsweise die Ausführung von „*Zertifikate zuweisen*“, eine zusätzliche Autorisierung, gilt dies dann auch für die Aktionen „*Zertifikate löschen*“, „*Zertifikate neu erstellen*“, „*Zertifikate importieren*“ etc.

Soll für eine dieser Aktionen eine zusätzliche Autorisierung notwendig sein, muss für diese Aktion auch angegeben werden, welche Anzahl von Security Officer hierfür notwendig sind.

Markieren Sie dazu die entsprechende Aktion. Ein Doppelklick auf die markierte Aktion öffnet einen Dialog, in dem die Anzahl der notwendigen Security Officer angegeben werden kann. Nach dem Klick auf **OK** wird die Liste im Reiter *Zusätzliche Autorisierung* innerhalb des Knotens **Zentrale Einstellungen** entsprechend aktualisiert.

Wird festgestellt, dass die erforderliche Anzahl an Security Officers mit entsprechenden Rechten nicht zur Verfügung steht, wird eine Meldung angezeigt, die Sie darauf hinweist.

Hinweis: Die Anzahl der tatsächlich zur Verfügung stehenden Security Officer kann zu diesem Zeitpunkt vom System nicht genau festgestellt werden. Bitte beachten Sie, dass möglicherweise die geforderte Anzahl nicht zur Verfügung steht, auch wenn diese Meldung nicht angezeigt wird. Das gilt beispielsweise dann, wenn globale Rechte der Security Officer später geändert wurden oder Security Officer gelöscht werden.

Achtung: Wenn Sie darauf hingewiesen werden, dass die erforderlichen Security Officer nicht zur Verfügung stehen, und Sie bei der Anzahl der notwendigen Security Officers angeben, dass mindestens ein zusätzlicher Security Officer notwendig ist, anschließend den Dialog mit OK bestätigen und schließen, wird die Einstellung aus technischen Gründen dennoch übernommen.

Dies führt dazu, dass die Aktionen, die eine zusätzliche Autorisierung verlangen, dann nicht mehr ausgeführt werden können, da die hierzu notwendigen Security Officer entweder nicht vorhanden sind oder diese nicht die erforderlichen Rechte besitzen. Wird eine solche Einstellung z. B. für die Option **Einstellungen für zusätzliche Autorisierung ändern** vorgenommen, kann keine Einstellung in diesem Dialog mehr geändert werden.

Die einzige Möglichkeit, diese Einstellung wieder zu ändern besteht noch darin, einen Wiederherstellungsschlüssel zu erzeugen (siehe *Zusätzliche Autorisierung aufheben* auf Seite *74*).

Eine vergleichbare Situation kann beim Löschen von Security Officers entstehen, da bei diesem Vorgang nicht geprüft wird, ob nach dem Löschen eines Security Officers noch die für eine zusätzliche Autorisierung notwendige Anzahl von Security Officers vorhanden ist. *u.trust LAN Crypt* stellt nur sicher, dass immer ein Master Security Officer im System vorhanden ist.

Hinweis: Wenn Sie keine Sicherheitstoken zur zusätzlichen Autorisierung benutzen, empfehlen wir, die **Option Hohe Sicherheit für den privaten Schlüssel** auf **Ja** einzustellen. Diese Einstellung können Sie auf dem Windows-Server über die *u.trust LAN Crypt* Gruppenrichtlinienverwaltung vornehmen.

Zusätzliche Autorisierung ausführen

Wurde für eine Aktion eine zusätzliche Autorisierung festgelegt, wird bei deren Aufruf ein Assistent für die zusätzliche Autorisierung gestartet. Dieser Assistent verlangt die Autorisierung durch mindestens einen weiteren Security Officer. Der betreffende Security Officer kann in einem Dialog ausgewählt werden.

War die Authentisierung dieses Security Officers über sein Zertifikat erfolgreich, kann die gewünschte Aktion ausgeführt werden.

Verwenden mehrere Security Officer dasselbe Zertifikat, kann dieses Zertifikat nur für einen einzigen Security Officer im Rahmen einer Autorisierungsaktion verwendet werden. Ein weiterer Security Officer, dem dieses Zertifikat ebenfalls zugeteilt ist, wird in der Liste der auswählbaren Security Officer dann nicht mehr angezeigt. Zum Ausführen von Autorisierungsaktionen müssen Security Officer daher immer über unterschiedliche Zertifikate verfügen.

Hinweis: Der Dialog zur Auswahl eines Security Officers enthält eine Option zur Anzeige der Security Officers einer bestimmten Region. Security Officers, die keiner Region zugeordnet sind, werden in der Liste immer angezeigt.

Autorisierung zurücksetzen

Eine zusätzliche Autorisierung für eine Aktion behält im Allgemeinen für die gesamte Dauer während einer Sitzung in der *u.trust LAN Crypt* Administration ihre Gültigkeit. Über das Symbol **Alle erteilten zusätzlichen Autorisierungen widerrufen** in der Symbolleiste der Administration können jedoch die entsprechenden Informationen gelöscht werden, sodass beim nächsten Ausführen der Aktion auch in derselben Sitzung erneut eine zusätzliche Autorisierung notwendig wird.

Zusätzliche Autorisierung aufheben

Falls Änderungen an der Konfiguration dazu führen sollten, dass nicht mehr genügend Security Officer vorhanden sind, um bestimmte Aktionen zu genehmigen, kann mithilfe des Wiederherstellungsschlüssels die Anzahl der zusätzlichen Security Officer, die eigentlich notwendig wären, um die Einstellungen für die zusätzliche Autorisierung zu ändern, wieder auf „0“ zurückgesetzt werden.

Klicken Sie hierzu im Anmeldedialog zur Datenbank auf die Schaltfläche **Zertifikat zuweisen**. Auf diese Weise starten Sie den Assistenten für den Wiederherstellungsschlüssel, mit dessen Hilfe Sie dann die Anzahl der notwendigen zusätzlichen Security Officers wieder auf „0“ zurücksetzen können.

3.5.10 Wiederherstellungsschlüssel

u.trust LAN Crypt sieht die Möglichkeit vor, einen Wiederherstellungsschlüssel zu generieren. Mithilfe dieses Schlüssels kann einem Master Security Officer bei der Anmeldung an die *u.trust LAN Crypt* Datenbank ein neues Zertifikat zugewiesen werden (über die Schaltfläche **Zertifikat zuweisen** im Anmeldedialog), wenn dieses z. B. beschädigt ist und deshalb nicht mehr genutzt werden kann. Mit dem Wiederherstellungsschlüssel kann auch die Anzahl der zusätzlichen Security Officer, die notwendig sind, um die Einstellungen für die zusätzliche Autorisierung zu ändern, auf „0“ zurückgesetzt werden.

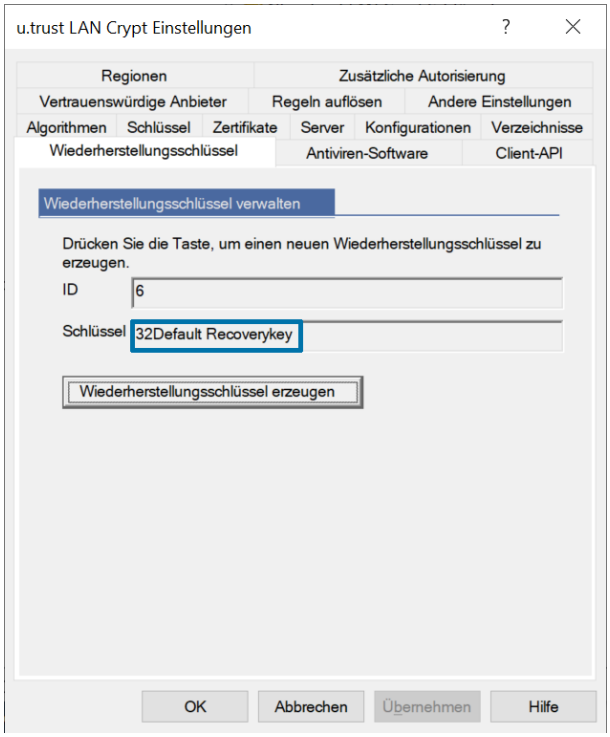
Ein Wiederherstellungsschlüssel kann in mehrere Teile aufgesplittet werden, und es kann festgelegt werden, wie viele Teile zum Zuweisen eines neuen Zertifikats notwendig sind. Die einzelnen Teile des Wiederherstellungsschlüssels können an verschiedene Security Officer verteilt werden. Die Besitzer der einzelnen Teile müssen bei der Verwendung des Wiederherstellungsschlüssels anwesend sein und über einen Assistenten die Teile des

Schlüssels präsentieren. Der Wiederherstellungsschlüssel bzw. dessen Teile können manuell eingegeben werden oder auch aus einer Datei geladen werden.

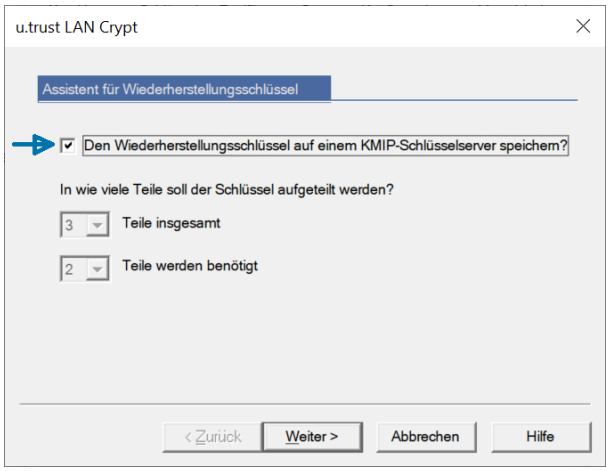
Alternativ können Sie aber (ab Version 4.1.0) den Wiederherstellungsschlüssel auch auf einem **KMIP-Schlüsselserver** speichern.

Hinweis: Mithilfe eines **KMIP-Schlüsselservers** (optional) können Sie den Wiederherstellungsschlüssel auf eine besonders sichere Weise speichern. Beachten Sie, dass von *u.trust LAN Crypt* derzeit nur der **Enterprise Secure Key Manager (ESKM)** des Herstellers *Utimaco* unterstützt wird.

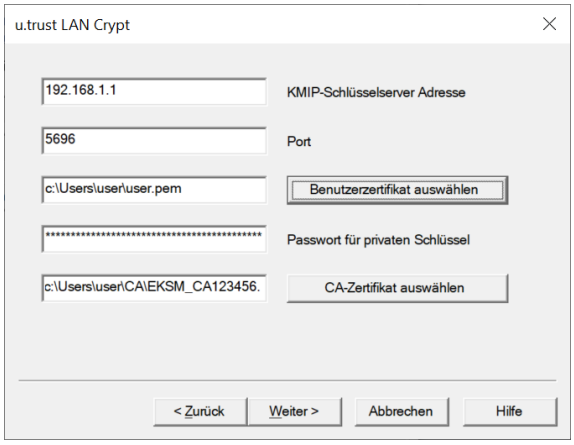
Zur Erzeugung eines Wiederherstellungsschlüssels öffnen Sie in der Admin-Konsole im Knoten **Zentrale Einstellungen** das Kontextmenü und klicken Sie dort auf *Eigenschaften.* Wechseln Sie im angezeigten Dialog zum Reiter **Wiederherstellungsschlüssel** und klicken Sie dann auf die Schaltfläche **Wiederherstellungsschlüssel erzeugen**. Der Assistent zur Erzeugung des Wiederherstellungsschlüssels wird gestartet.



Aktivieren Sie entweder die Option **Den Wiederherstellungsschlüssel auf einem KMIP-Schlüsselserver speichern?** oder wählen Sie über die Dropdownmenüs aus, aus wie vielen Teilen der Schlüssel bestehen soll und wie viele Teile davon für eine Verwendung des Wiederherstellungsschlüssels notwendig sind.

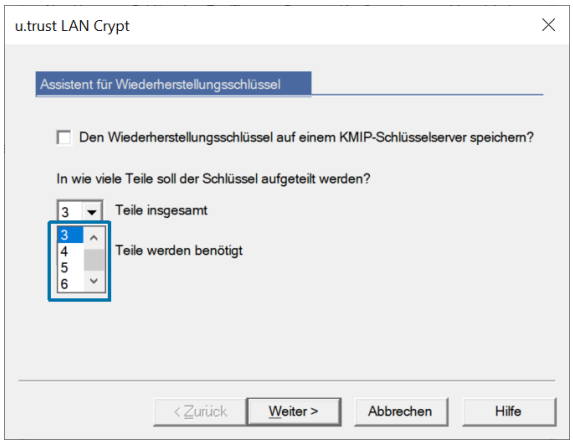


Wenn Sie die Option **Den Wiederherstellungsschlüssel auf einem KMIP-Schlüsselserver speichern?** gewählt haben und dann auf **Weiter** klicken, müssen Sie die Verbindungsdaten für den **KMIP-Schlüsselserver** (*Serveradresse* und *Port*) sowie die erforderlichen Zertifikatsangaben sowie das Passwort für den privaten Schlüssel in die jeweiligen Eingabefelder eintragen.



Klicken Sie danach auf **Weiter**. Die Verbindung zum **KMIP-Schlüsselserver** sowie die Zertifikatsangaben werden geprüft und bei Erfolg der Wiederherstellungsschlüssel auf sichere Weise auf dem **KMIP-Schlüsselserver** gespeichert.

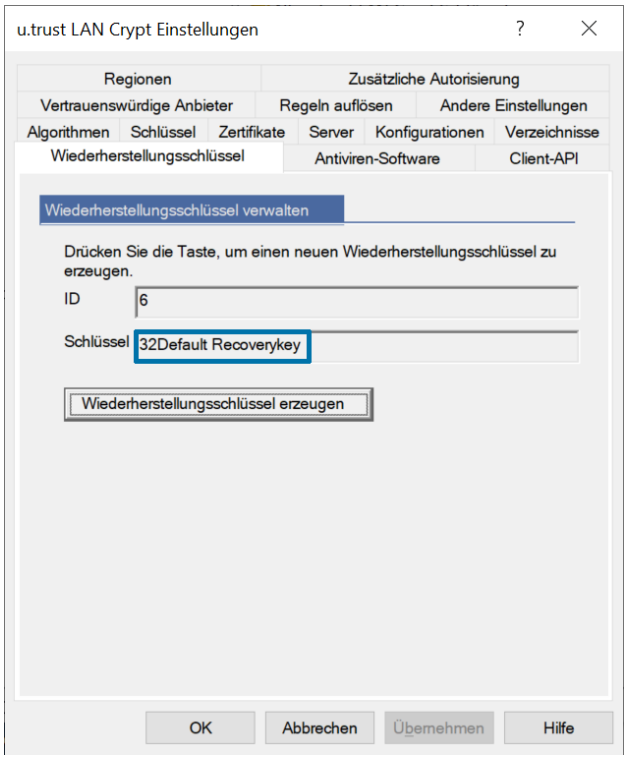
In unserem Beispiel soll der Schlüssel aus drei Teilen bestehen, wobei mindestens zwei davon für das Zuweisen eines neuen Security Officer Zertifikats bei der Anmeldung notwendig sind.



Wählen Sie über die Dropdownmenüs aus, aus wie vielen Teilen der Schlüssel bestehen soll und wie viele Teile davon für eine Verwendung des Wiederherstellungsschlüssels notwendig sind. In unserem Beispiel soll der Schlüssel aus drei Teilen bestehen, wobei mindestens zwei davon für das Zuweisen eines neuen Security Officer Zertifikats bei der Anmeldung notwendig sind. Klicken Sie auf **Weiter**.

Der Assistent zeigt für jeden Teil des Schlüssels einen Dialog an, in dem Sie auswählen können, ob der Teilschlüssel in einer Datei gespeichert wird, oder ob er angezeigt werden soll. Wenn alle Teile abgearbeitet wurden, wird der Assistent geschlossen.

Im Reiter **Wiederherstellungsschlüssel** wird unten in der Tabelle direkt links neben dem Eintrag „*Default Recoverykey*“ angezeigt, aus wie vielen Teilen der Schlüssel besteht (im genannten Beispiel sind es 3 Teile) und wie viele Teile von diesen bei der Verwendung notwendig sind (im genannten Beispiel sind es 2).



Hinweis: Bitte beachten Sie bei der Erzeugung und dem Verteilen der Teile des Wiederherstellungsschlüssels, dass es sich dabei um äußerst sensible Daten handelt. Der Wiederherstellungsschlüssel muss unbedingt vor Unbefugten geschützt werden.

Achtung: Es kann immer nur der letzte erzeugte Wiederherstellungsschlüssel verwendet werden! Alle zuvor erzeugten Schlüsselteile sind dann nicht mehr gültig und können somit nicht mehr zum Zuweisen eines Zertifikats verwendet werden.

Verwenden des Wiederherstellungsschlüssels

Sollte eine Anmeldung an die *u.trust LAN Crypt*-Datenbank nicht mehr möglich sein (z. B., weil das Zertifikat abgelaufen ist), klicken Sie im Dialog zur Auswahl des Security Officers auf die Schaltfläche **Zertifikat wechseln**, um den Assistenten für den *Wiederherstellungsschlüssel* zu starten.

Sollten Sie nach der Auswahl eines Security Officers zur Anmeldung durch einen Dialog darauf hingewiesen werden, dass das Zertifikat nicht mehr gültig ist, können Sie den Assistenten direkt von dort aus starten.

Folgen Sie den Anweisungen des Assistenten.

Je nachdem, welche Einstellung für den Wiederherstellungsschlüssel gewählt wurde (entweder klassisch oder über einen **KMIP-Schlüsselserver**), zeigt der Assistent den jeweils

erforderlichen Dialog an, um für den (Master) Security Officer ein neues Zertifikat zu erstellen, um diesem den Zugang zur *u.trust LAN Crypt* Administration wieder zu ermöglichen.

In diesem Assistenten ist auch ein Dialog enthalten, der Ihnen die Möglichkeit bietet, die Anzahl der Security Officer, die nötig sind, um die Einstellungen für eine zusätzliche Autorisierung zu ändern, wieder zurück auf „0“ zu setzen.

Durch diesen Mechanismus ist sichergestellt, dass nie eine Situation entstehen kann, in der keine zusätzliche Autorisierung mehr möglich ist, weil beispielsweise hierfür notwendige Security Officer nicht mehr vorhanden sind.

Wenn Sie diese Option aktivieren, kann anschließend ein einzelner Security Officer die Einstellungen für die zusätzliche Autorisierung ändern.

3.5.11 Datenbank

Hinweis: Diese Einstellung ist nur bei der Verwendung einer Oracle-Datenbank notwendig, auf die von verschiedenen Administrationsstationen zugegriffen wird. Sie kann nur von einem Master Security Officer vorgenommen werden.

Der **N**ational **L**anguage **S**upport (NLS) von Oracle konvertiert Texte in der Form, dass Texte unabhängig vom eingestellten Zeichensatz für den Anwender immer gleich dargestellt werden, auch wenn sie aufgrund des zugrunde liegenden Zeichensatzes numerisch unterschiedlich codiert werden (Beispiel: WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00).

Werden Texte in die Datenbank eingefügt und basierend auf einem anderen Zeichensatz ausgelesen (Zeichen werden konvertiert, binäre Daten wie MAC nicht), führt dies dazu, dass bei der Berechnung der Prüfsumme (MAC)-Fehler auftreten.

Um diese Fehler zu vermeiden, sollte sichergestellt werden, dass auf allen Administrations-stationen, auf die über den Oracle-Client auf die Datenbank zugegriffen wird, dieselbe Code Page / derselbe Zeichensatz verwendet wird.

Dazu kann auf der Seite *Datenbank* ein Zeichensatz angegeben werden, der von allen Administrationsstationen verwendet werden muss, die auf die Datenbank zugreifen. Beim Start der Admin-Konsole prüft *u.trust LAN Crypt*, ob die Einstellung des Oracle-Clients mit der Einstellung in der Administration übereinstimmt. Ist dies nicht der Fall, wird eine Warnung angezeigt und die *u.trust LAN Crypt* Administration wird nicht gestartet.

Geben Sie im Eingabefeld den Zeichensatz an, der auf den Oracle-Clients angegeben sein muss, damit sich diese an die *u.trust LAN Crypt* Administration anmelden dürfen. Auf den Oracle-Clients finden Sie diese Einstellung in der Windows Registrierung unter dem Wert `NLS_Lang` (`Language.Territory.CharacterSet`. Beispiel: `GERMAN_GERMANY.`**`WE8MSWIN1252`**).

Der Zeichensatz der aktuellen Maschine wird unter *INFO*: im Reiter **Datenbank** angezeigt. Dieser sollte möglichst auch von allen anderen Clients verwendet werden, die auf die Datenbank zugreifen.

Hinweis: Wir empfehlen Ihnen, nur einen Zeichensatz zu verwenden! Wenn Sie mehr als einen Zeichensatz verwenden, dann können Fehler beim Errechnen der Prüfsumme (MAC) auftreten. Prinzipiell ist es aber möglich, mehrere Zeichensätze anzugeben. Von dieser Möglichkeit sollte aber ausschließlich nur dann Gebrauch gemacht werden, wenn es sich hierbei um Zeichensätze handelt, die weitgehend identisch sind und sich nur bei wenigen Zeichen unterscheiden. Diese unterschiedlichen Zeichen sollten bekannt sein und dürfen dann für Einträge in die Datenbank nicht verwendet werden!

Deaktivierung der Prüfung

u.trust LAN Crypt bietet die Möglichkeit, die Prüfung der verwendeten Character Sets zu deaktivieren. Wird das Eingabefeld leer gelassen, findet keine Prüfung statt und die Anmeldung wird immer erlaubt. Bitte beachten Sie, dass dies zu Fehlern bei der Berechnung der Prüfsumme (MAC) führen kann.

Um mögliche Fehler (z. B. Tippfehler) bei der Angabe eines Zeichensatzes zu verhindern, die dazu führen können, dass sich auch der Master Security Officer, der die Einstellung selbst vorgenommen hat, nicht mehr an der Admin-Konsole anmelden kann, wird die Eingabe beim Klicken auf **Übernehmen** bzw. **OK** nochmals geprüft. Entspricht die angegebene Einstellung nicht dem derzeit auf dieser Arbeitsstation gültigen Zeichensatz, wird eine entsprechende Meldung angezeigt und der aktuell gültige Zeichensatz wird zusätzlich in das Eingabefeld eingefügt. Das Register **Datenbank** bleibt geöffnet, sodass die eingegebenen Daten noch einmal geprüft werden können. Ändern Sie gegebenenfalls die Einstellung und klicken Sie erneut auf **Übernehmen** bzw. **OK**.

3.5.12 Antiviren-Software

Damit Virenscanner in der Lage sind, auch mit *u.trust LAN Crypt* verschlüsselte Dateien zu scannen, müssen Anwendungen in diesem Register angegeben werden. Die dort eingetragene Antiviren-Software wird somit explizit für den Zugriff auf verschlüsselte Dateien autorisiert und kann beim Scanvorgang Virensignaturen auch in *u.trust LAN Crypt* verschlüsselten Dateien erkennen.

Um einen Virenscanner hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie die folgenden Daten in das angezeigte Dialogfeld ein:

- Einen beliebigen Namen für die Antiviren-Software (dieser Name wird in der Tabelle in im Register **Antiviren-Software** in der Spalte *Produkt* angezeigt).
- Den Namen der ausführbaren Datei, die den Virenscan ausführt.

Um zu verhindern, dass Virenscanner den Ladevorgang der *u.trust LAN Crypt* Client Profildatei verlangsamen, konfigurieren Sie die Antiviren-Prozesse so, dass diese entweder bereits aktiv sind, wenn die Client-Verschlüsselungsregeln geladen werden oder geben Sie den Pfad zur ausführbaren Datei (*EXE-Dateiname*) mit an, die den Virenscan ausführt. Sie können innerhalb des Pfades auch Platzhalter verwenden.

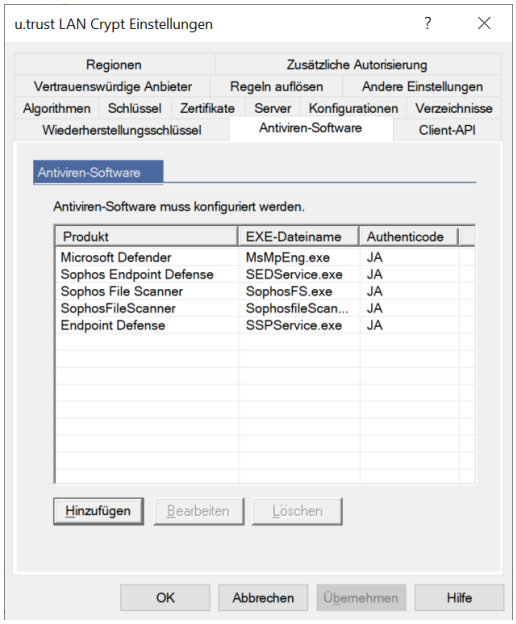
Beispiel:

```
C:\ProgramData\Microsoft\Windows Defender\Platform\*\MsMpEng.exe
```

Aktivieren Sie die Option **Authenticode-Verifizierung verwenden**.

Hinweis: Wir empfehlen, unbedingt einen Authenticode-signierten Virenscanner zu verwenden, diesen hier einzutragen und die *Authenticode-Verifizierung* zu aktivieren. Nur durch diese Verifizierung kann sichergestellt werden, dass es sich um die gewünschte ausführbare Datei des Virenscanners handelt und damit ausschließlich vertrauenswürdige Anwendungen den explizit gewünschten Zugriff auf verschlüsselte Dateien erhalten.

Nach einem Klick auf **OK** wird die Antiviren-Software in der Liste angezeigt. Sie können auch noch weitere Virenscanner hinzufügen.



3.5.13 Client-API

u.trust LAN Crypt stellt eine Client-API zur Verfügung, die es Anwendungen erlaubt, die Dateiverschlüsselungsfunktionalität über eine einfache Kommandozeile oder eine COM-style-API zu steuern. Details dazu finden Sie in der Client-API-Dokumentation im Ordner `\api` Ihres entpackten Installationspakets.

Hinweis: Die API muss während der Installation des *u.trust LAN Crypt* Clients ausgewählt werden. Wenn Sie die Client-API auf Ihren Clients verwenden wollen, dann stellen Sie sicher, dass diese korrekt installiert ist.

Geben Sie dazu in im Register **Client-API** die Einstellungen für die Client-API an.

- Wählen Sie **Client-API aktivieren**, um die API auf dem Client verfügbar zu machen. Nun können Anwendungen die Dateifunktionalität über die COM-style-API steuern.
- Wählen Sie **API-Zugriff für das u.trust LAN Crypt Dateiverschlüsselungs-Kommandozeilen-Tool aktivieren**, um die Steuerung der Dateiverschlüsselungsfunktion über ein einfaches Kommandozeilenwerkzeug zu ermöglichen.

- **API-Regeln haben Vorrang gegenüber Verschlüsselungsregeln in Profilen**. Standardmäßig haben Verschlüsselungsregeln, die in der *u.trust LAN Crypt* Administration definiert sind, Priorität vor Verschlüsselungen, die über die Client-API ausgeführt werden. Wenn Sie jedoch die API-Regeln priorisieren wollen, wählen Sie die Option **API-Regeln haben Vorrang gegenüber Verschlüsselungsregeln in Profilen**.

  Anmerkung: Die *u.trust LAN Crypt* **Ignorieren Regeln** und **Ausschließen-Regeln** haben stets höchste Priorität und können daher nicht durch API-Regeln außer Kraft gesetzt werden, da in diesen Fällen die Verschlüsselung schon automatisch ausgeschlossen wird (siehe „*Von einer Verschlüsselung ausgenommene Dateien und Ordner*“ auf Seite 10).

Da der API-Zugang nur auf erlaubte Anwendungen beschränkt ist, müssen Sie diese Anwendungen angeben.

1. Klicken Sie auf **Hinzufügen** im Register **Client-API**.
2. Geben Sie an, welche Anwendung die Client-API verwenden darf.
3. Geben Sie den Namen der ausführbaren Datei an, die auf die API zugreifen soll.
4. Wenn Sie wollen, dass nur Authenticode-signierte ausführbare Dateien auf die API zugreifen sollen, wählen Sie die Option **Ausführbare Datei muss Authenticode-signiert sein**.
5. Wenn Sie nur ausführbare Dateien verwenden wollen, die von vertrauenswürdigen Anbietern signiert sind, wählen Sie die Option **Ausführbare Datei muss von einem vertrauenswürdigen Anbieter Authenticode-signiert sein**. Damit stellen Sie sicher, dass nur ausführbare Dateien zugelassen werden, die ein Zertifikat verwenden, das im *Signaturzertifikat* eines Anbieters registriert ist und auch im Register **Vertrauenswürdige Anbieter** eingetragen ist.
6. Geben Sie optional einen Kommentar ein.

Nach Klicken auf **OK** erscheint die Anwendung in der Liste. Sie können weitere Anwendungen hinzufügen.

3.5.14 Vertrauenswürdige Anbieter

Im Register **Vertrauenswürdige Anbieter** können Sie Anbieter eintragen, die mit einer Authenticode-signierten ausführbaren Datei auf die Client-API zugreifen dürfen.

Zum Hinzufügen eines vertrauenswürdigen Anbieters

1. klicken Sie auf **Hinzufügen** im Register **Vertrauenswürdige Anbieter**.
2. Geben Sie den Namen des Anbieters ein.
3. Geben Sie das Signaturzertifikat des Anbieters ein.

   Sofern dies im Register **Client-API** definiert ist, werden von der API nur ausführbare Dateien (Anwendungen) akzeptiert, die mit diesem Zertifikat Authenticode-signiert sind.
4. Geben Sie optional einen Kommentar ein.

Nach Klicken auf **OK** erscheint der Anbieter in der Liste. Sie können weitere Anbieter hinzufügen.

3.5.15 Andere Einstellungen

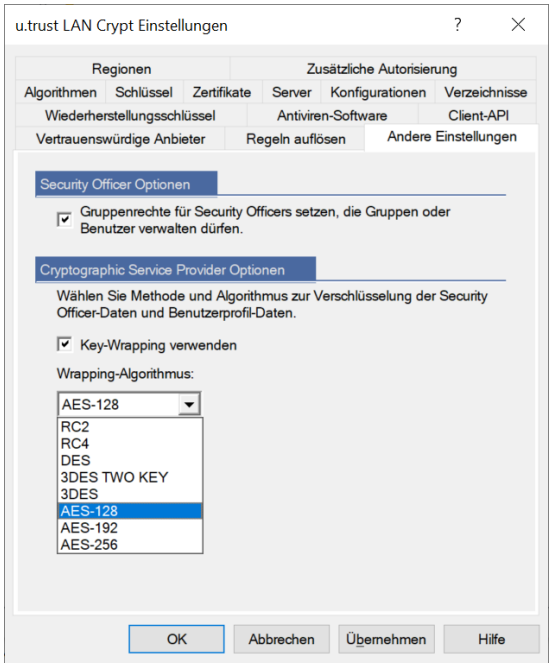
Security Officer-Optionen

u.trust LAN Crypt kann so konfiguriert werden, dass automatisch eine ACL mit Leserecht für die Stammgruppe für einen neu erstellten Security Officer erzeugt wird. Hierfür ist erforderlich, dass der Security Officer das globale Recht *Gruppen verwalten* oder *Benutzer verwalten* hat. Dadurch wird garantiert, dass der Security Officer den erforderlichen Zugriff (einsehen und / oder bearbeiten) auf alle Gruppen hat. Aktivieren Sie hierzu die Option **Gruppenrechte für Security Officers setzen, die Gruppen oder Benutzer verwalten dürfen**.

Hinweis: Wenn Sie danach einen Security Officer aus Gruppen entfernen wollen, ist dies nur in der Stammgruppe möglich, d. h. im Hauptknoten **Gruppen**, da die Berechtigungen auf alle darunterliegenden Untergruppen „vererbt“ werden.

Cryptographic Service Provider Optionen

Wenn Sie die Option **Key-Wrapping verwenden** (Standardeinstellung) aktivieren, werden Security Officer-Daten und Benutzerprofildaten mit einem per Zufallsverfahren erzeugten Session-Key mit dem ausgewählten Algorithmus (Standard: AES) verschlüsselt. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel aus dem Zertifikat RSA-verschlüsselt.



Wenn Sie Smartcards verwenden, stellen Sie sicher, dass diese bzw. die in diesem Zusammenhang verwendete Middleware auch den von Ihnen ausgewählten Algorithmus unterstützt. Ist dies nicht der Fall, wählen Sie alternativ einen anderen kompatiblen Algorithmus.

Wenn Sie diese Option deaktivieren, werden die Daten ohne einen solchen Session Key, RSA-verschlüsselt. Beachten Sie, dass Smartcards bzw. die eingesetzte Middleware diese Option unter Umständen nicht unterstützen.

Hinweis: Wird der gewählte Algorithmus nicht unterstützt, erhalten die Benutzer beim Laden der Profildatei eine entsprechende Fehlermeldung. Ändern Sie in dem Fall den Algorithmus bzw. wählen Sie einen passenden Algorithmus, den die von Ihnen eingesetzte Smartcard bzw. Middleware unterstützt.

3.6 Alle u.trust LAN Crypt Schlüssel anzeigen

Über den Knoten **Alle u.trust LAN Crypt Schlüssel** in der *u.trust LAN Crypt* Admin-Konsole können Sie sich einen Überblick über sämtliche von *u.trust LAN Crypt* verwalteten Schlüssel verschaffen. Sie bekommen dabei folgende Informationen angezeigt:

- Langer Schlüsselname
- Den für den Schlüssel verwendeten Algorithmus
- Information darüber, ob der Schlüssel aktiv ist
- Wer den Schlüssel erzeugt hat (Ersteller)
- Information darüber, ob der Schlüssel vererbt wurde
- Für welche Gruppe der Schlüssel erzeugt wurde
- Information darüber, ob der Schlüssel in Verwendung ist
- Kommentarfeld

Durch Klicken auf den Kopf einer Spalte können Sie die Tabelle auf- oder absteigend nach der gewünschten Information sortieren lassen.

In der Standard-Ansicht werden zunächst alle erstellten Schlüssel der jeweiligen Gruppen angezeigt. Durch Klicken mit der rechten Maustaste auf den Knoten **Alle u.trust LAN Crypt Schlüssel**, können Sie über das Kontextmenü die Schlüsselanzeige im rechten Fenster ändern und sich so z. B. auch die spezifischen Schlüssel, wie beispielsweise alle vorhandenen Gruppen- (<GROUPKEY>) und Benutzerschlüssel (<USERKEY>) anzeigen lassen.

3.6.1 Schlüssel finden

Zusätzlich zum Sortieren der Schlüsselinformationen besteht die Möglichkeit, einen bestimmten Schlüssel suchen zu lassen. Klicken Sie dazu mit der rechten Maustaste auf den Knoten **Alle u.trust LAN Crypt Schlüssel** und wählen Sie dann aus dem Kontextmenü den Eintrag *Schlüssel finden*.

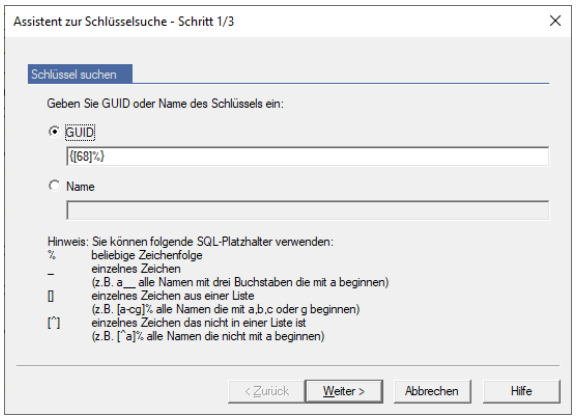
Hinweis: Die Funktion **Schlüssel finden** steht auch für den Knoten **Gruppenschlüssel** in jeder Gruppe zur Verfügung. Zum Hinzufügen eines Schlüssels zu einer Gruppe muss ein Security Officer auch das Recht *Schlüssel kopieren* für die Gruppe, in der sich der Schlüssel befindet und das Recht *Schlüssel erzeugen* für die Gruppe, zu der dieser Schlüssel hinzugefügt werden soll, besitzen.

Anschließend wird ein Assistent aufgerufen, der Sie beim Suchen des gewünschten Schlüssels unterstützt. In Schritt 1 können Sie angeben, ob Sie nach der GUID oder dem

Namen eines Schlüssels suchen möchten. Sie können hierfür bestimmte SQL-Platzhalter verwenden.

Beispiel:

{[68]%} liefert alle Schlüssel, deren GUIDs mit 6 oder 8 beginnen.



Klicken Sie anschließend auf **Weiter**, um in der Datenbank nach dem gewünschten Schlüssel zu suchen. Wurde der Schlüssel gefunden, erhalten Sie in Schritt 2 den Schlüsselnamen, die GUID des Schlüssels und die Gruppe angezeigt, in welcher der Schlüssel erzeugt wurde.

Haben Sie die Funktion **Schlüssel finden** über den Gruppenschlüsselknoten einer Gruppe aufgerufen, können Sie durch Aktivieren der Option **Schlüssel der aktuellen Gruppe zuordnen** einen Verweis auf den gefundenen Schlüssel erzeugen. Sie sind dann in der Lage, den in einer anderen Gruppe erzeugten Schlüssel in der aktuell ausgewählten Gruppe zu verwenden. Wenn Sie die Option aktivieren, auf **Weiter** klicken und anschließend in Schritt 3 auf **Beenden**, erhalten Sie im Knoten **Gruppenschlüssel** der dazugehörigen aktuellen Gruppe ein spezielles Schlüsselsymbol angezeigt. Sie können diesen Schlüssel nun in Verschlüsselungsregeln einsetzen.

Hinweis: Das Auswählen der Option **Schlüssel der aktuellen Gruppe zuordnen** wirkt sich nur aus, wenn Sie die Funktion **Schlüssel finden** über den Knoten **Gruppenschlüssel** einer Gruppe aufgerufen haben und nicht über den Knoten **Alle u.trust LAN Crypt Schlüssel**. Sie können auch spezifische Schlüssel auswählen; diese werden der aktuellen Gruppe jedoch nicht zugeordnet. Wenn Ihre Auswahl einen spezifischen Schlüssel enthält, so erscheint auf der letzten Seite des Assistenten eine entsprechende Meldung.

3.7 Ausgewählte Benutzer und Zertifikate anzeigen

Der Knoten **Ausgewählte Benutzer und Zertifikate** steht nur zur Verfügung, wenn in den Benutzereinstellungen der **u.trust LAN Crypt Administration** die Option *„Ausgewählte Benutzer und Zertifikate anzeigen“* aktiviert ist (siehe *„Benutzereinstellungen“* auf Seite 49).

Wenn Sie auf den Knoten **Ausgewählte Benutzer und Zertifikate** klicken, erscheint ein Dialog, in dem Sie auswählen können, ob alle oder nur bestimmte Benutzer angezeigt werden sollen. Da das Anzeigen aller Benutzer sehr zeitaufwendig werden kann, ermöglicht *u.trust LAN Crypt* das Einschränken der Suche durch die Definition von Suchkriterien.

Hinweis: Ist eingestellt, dass die Benutzerlisten zwischengespeichert werden (Standardeinstellung), müssen Sie die Anzeigen entweder über das Symbol in der Symbolleiste oder durch Drücken von **F5** zuerst aktualisieren, bevor Sie neue Suchkriterien angeben können.

Durch Auswählen der Option *Passende Benutzer anzeigen* werden die Eingabefelder zum Festlegen der Suchkriterien aktiviert.

Folgende Informationen über die Benutzer werden aus der *u.trust LAN Crypt* Datenbank ermittelt:

- Anmeldename
- Benutzername
- Zuordnung zwischen Benutzer und Zertifikat
- Antragssteller des Zertifikats
- Datum, ab wann das Zertifikat gültig ist
- Datum, bis wann das Zertifikat gültig ist
- Aussteller des Zertifikats
- Namen des Elternelements

Basierend auf diesen Attributen können die Suchkriterien angegeben werden. *u.trust LAN Crypt* sucht nach festgelegten Zeichenketten in den ausgelesenen Attributen der Benutzer.

In der ersten Dropdownliste können Sie auswählen, auf welche(s) Attribut(e) die Suche angewendet werden soll.

Daneben können Sie festlegen, ob die Zeichenkette enthalten sein soll (*soll sein*) oder ob nur Benutzer angezeigt werden, in denen die Zeichenkette im ausgewählten Attribut nicht enthalten sein darf (*darf nicht sein*).

In der Dropdownliste ganz rechts können Sie die eigentliche Zeichenkette, die *u.trust LAN Crypt* im angegebenen Attribut sucht, eingeben.

Zur Angabe der Zeichenkette können Sie folgende SQL-Platzhalter verwenden:

%	beliebige Zeichenfolge
_	einzelnes Zeichen (z.B. a__ bedeutet suche nach allen Namen mit drei Buchstaben, die mit „a“ beginnen)
[ ]	einzelnes Zeichen aus einer Liste (z. B. [a-cg]% bedeutet suche nach allen Namen, die mit „a,b,c“ oder „g“ beginnen)
[^]	einzelnes Zeichen, das nicht in einer Liste ist (z. B. [^a]% bedeutet suche nach allen Namen, die mit „a“ beginnen)

Sie können bis zu drei Bedingungen für die Suche angeben.

Geben Sie mehr als eine Bedingung an, können Sie festlegen, wie diese Bedingungen verknüpft werden sollen (UND / ODER).

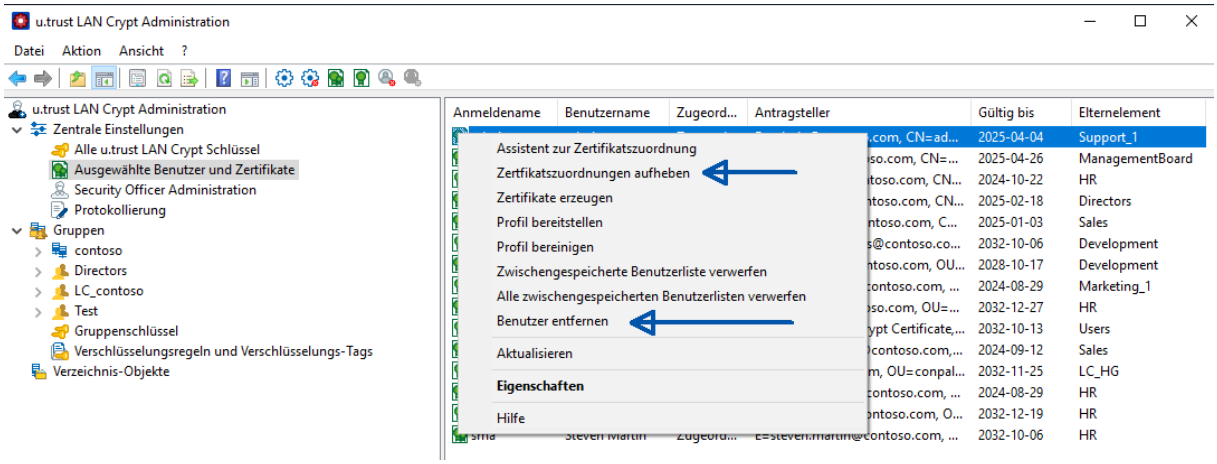
Über einen Klick mit der rechten Maustaste auf den Knoten **Ausgewählte Benutzer und Zertifikate** können Sie alle Funktionen des Zertifikat-Snap-Ins nutzen, die auch für jede einzelne Gruppe verfügbar sind (siehe „*Zuordnung der Zertifikate*“ auf Seite 157).

Der Assistent zur Zertifikatszuordnung steht an dieser Stelle nur einem Master Security Officer zur Verfügung. Ein Security Officer kann, sofern er die entsprechenden Rechte besitzt, einem einzelnen Benutzer über das *Eigenschaften*-Menü ein Zertifikat zuweisen.

Besitzt ein Security Officer nicht die erforderlichen Rechte für den dargestellten Benutzer, wird ein entsprechendes Symbol angezeigt.

3.7.1 Die Funktionen „Zertifikatszuweisungen aufheben“ und „Benutzer entfernen“

Für die im rechten Dialogfeld angezeigten Benutzer im Knoten **Ausgewählte Benutzer und Zertifikate** stehen Ihnen über das Kontextmenü die Funktionen **Zertifikatszuweisungen aufheben** und **Benutzer entfernen** zur Verfügung, wenn Sie einen oder mehrere Benutzer markieren. Wurde einem Benutzer noch kein Zertifikat zugewiesen, erkennen Sie das daran, dass sein Benutzersymbol „grau“ angezeigt wird. Benutzer, die bereits über ein gültiges Zertifikat verfügen, können Sie daran erkennen, dass deren Benutzersymbol „grün“ angezeigt wird.



Die Funktion **Zertifikatszuordnungen aufheben**

Das Menüelement **Zertifikatszuordnungen aufheben** steht nur bei Benutzern mit grünem, gelbem oder rotem Benutzersymbol zur Verfügung. Mit „Zertifikatszuordnungen aufheben“ können Sie die Zuweisung von Zertifikaten für die zuvor markierten Benutzer aufheben. Danach ändert sich die Farbe des Benutzersymbols bei diesen Benutzern nach „grau“ und ihnen ist dann kein Zertifikat mehr zugewiesen.

Hinweis: Ein Benutzer kann auch mehrere Zertifikate besitzen. Mit **Zertifikatszuordnungen aufheben** werden alle dem Benutzer zugewiesenen Zertifikate aufgehoben. Bevor Sie einem solchen Benutzer ein neues Profil bereitstellen können, müssen Sie diesem zuerst ein Zertifikat zuweisen.

Hinweis: Wird die Farbe des Benutzersymbols in „rot“ angezeigt, bedeutet dies, dass das Zertifikat dieses Benutzers abgelaufen ist. Ist dagegen die Farbe des Benutzersymbols „gelb“, bedeutet dies, dass das Zertifikat des betroffenen Benutzers bald ablaufen wird (innerhalb der konfigurierten Warnfrist).

Die Funktion **Benutzer entfernen**

Mit **Benutzer entfernen**, können Sie einen vorhandenen Benutzer aus der *u.trust LAN Crypt* Datenbank löschen. Nachdem Sie **Benutzer entfernen** ausgeführt haben, wird der Benutzer nicht mehr im Knoten **Ausgewählte Benutzer und Zertifikate** und auch in den allen **Gruppen**, denen angehörte, nicht mehr angezeigt.

3.8 Anlegen eines Security Officers

Master Security Officer und Security Officer, die dazu berechtigt sind, können weitere Security Officer anlegen. Diese Security Officer können dann einzelnen Organisationseinheiten (Regionen) zugeordnet werden. Sie werden in einem ersten Schritt mit globalen Rechten (Rollen-basiert) ausgestattet, die exakt definieren, welche Aufgaben sie generell übernehmen dürfen. Werden Security Officer einer *u.trust LAN Crypt* Gruppe zugeordnet, können deren Rechte an diesem speziellen Objekt noch einmal über ACLs eingeschränkt werden.

Hinweis: Fehlt einem Security Officer im Rahmen seiner definierten globalen Rechte die Erlaubnis für eine bestimmte Aktion, kann ihm dieses fehlende Recht auch über eine ACL nicht mehr zugestanden werden.

1. Neue Security Officer werden in der Admin-Konsole unter dem Knoten **Security Officer Administration** angelegt. Durch Klicken auf **Neuen SO hinzufügen** im Kontextmenü dieses Knotens oder durch Klicken auf **Neuen SO hinzufügen** im Menü *Aktion*, wird der erste Dialog zum Hinzufügen eines neuen Security Officers geöffnet.

2. Geben Sie in diesem Dialog einen Namen und optional eine E-Mail-Adresse und einen Kommentar für den neuen Security Officer ein. Klicken Sie dann auf **Weiter**.

   Hinweis: Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von *u.trust LAN Crypt* erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN-Mailers, wie z. B. über das Tool „*LCSendP12Password*“, via E-Mail verwendet werden.

3. Geben Sie in diesem Dialog an, ob der neue Security Officer mit den Rechten für einen Master Security Officer ausgestattet sein soll. Ein Master Security Officer besitzt immer alle zur Verfügung stehenden Rechte. Wählen Sie über die **Suchen**-Schaltfläche ein vorhandenes Verschlüsselungszertifikat aus, oder erzeugen Sie über *u.trust LAN Crypt* ein neues Zertifikat für den Security Officer.

   Zertifikate über eine LDAP-Quelle zuordnen

   u.trust LAN Crypt ermöglicht die Zuordnung von Zertifikaten aus einem Microsoft Active Directory oder über LDAP-Quellen.

   Markieren Sie dafür **LDAP** in der Drop-Down-Liste des Dialogs *Wählen Sie ein Zertifikat*.

   Es wird jetzt ein Eingabefeld angezeigt, in das Sie die URL der LDAP-Quelle eingeben können. Nach Klicken auf **Aktualisieren** wird der Inhalt der LDAP-Quelle angezeigt. Begriffe in eckigen Klammern (z. B. *[Sub_OU1]*) bezeichnen die OUs in der LDAP-Quelle. Ein Doppelklick auf eine OU zeigt die darin enthaltenen Zertifikate an.

   Doppelklicken Sie auf [..], um in der Organisationsstruktur eine Ebene höher zu gelangen.

   Wählen Sie ein Zertifikat aus und klicken Sie auf **OK**. Das Zertifikat wird dem Security Officer zugewiesen.

   Hinweis: Wenn auf den LDAP-Server nicht über eine Anonymous-Anmeldung zugegriffen werden kann, müssen die Anmeldedaten im Register **Server** im Knoten **Zentrale Einstellungen** eingetragen werden.

Hinweis: Wenn Sie *u.trust LAN Crypt* ein Verschlüsselungszertifikat erzeugen lassen, muss dieser Security Officer den privaten Schlüssel aus der erzeugten „*.p12*"-Schlüsseldatei auf seiner Arbeitsstation importieren.

Wenn das Verschlüsselungszertifikat aus einem LDAP-Verzeichnis zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Security Officers vorhanden sein. Verschlüsselungszertifikate von Security Officers werden für den kryptografischen Zugriff auf die symmetrischen Datenbankschlüssel benötigt.

4. Wählen Sie optional über die zweite **Suchen ...**-Schaltfläche ein vorhandenes Signaturzertifikat aus, oder lassen Sie von *u.trust LAN Crypt* ein neues Zertifikat erzeugen.

   Hinweis: Wenn Sie *u.trust LAN Crypt* ein Signaturzertifikat erzeugen lassen, muss dieser Security Officer den privaten Schlüssel aus der erzeugten „*.p12*"- Schlüsseldatei auf seiner Arbeitsstation importieren.

   Wenn das Signaturzertifikat aus einem LDAP-Verzeichnis zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Security Officers vorhanden sein. Das Signaturzertifikat wird für die Signatur in den erzeugten Profildateien und für die Authentisierung im Rahmen des erweiterten API-Logons verwendet.

5. Insofern Sie auch Regionen für Ihre Security Officer definiert haben, können Sie jetzt eine Region auswählen.

6. Wenn Sie individuelle Konfigurationssätze für Regionen erstellt haben, können Sie jetzt einen hiervon auswählen.

   Hinweis: Es werden immer nur jene Konfigurationen angezeigt, die für die eingestellte Region erzeugt wurden.

7. Klicken Sie auf **Weiter**.

8. Im letzten Dialog des Assistenten können Sie festlegen, welche Aktionen der neue Security Officer durchführen darf. Wenn Sie eine Aktion auswählen, werden automatisch alle hierfür notwendigen globalen Rechte gesetzt. Diese Rechte werden unter den Eigenschaften des Security Officers (diese werden durch einen Doppelklick auf den Security Officer angezeigt) auf der Registerseite *Globale Rechte* angezeigt. Die globalen Rechte können an dieser Stelle angepasst werden.

   Wenn Sie dem Security Officer das Ausführen einer bestimmten Aktion in diesem Dialog erlauben, ist sichergestellt, dass er alle für diese Aktion notwendigen globalen Rechte erhält.

Wenn ein neuer Security Officer auf diese Weise die globale Berechtigung *Gruppen verwalten* oder *Benutzer verwalten* erhält, erstellt *u.trust LAN Crypt* automatisch eine ACL mit Leserechten für die Stammgruppe für diesen Security Officer, vorausgesetzt, dass die Option *Gruppenrechte für Security Officer setzen, die Gruppen oder Benutzer verwalten dürfen*, aktiviert ist. Dadurch wird garantiert, dass der Security Officer Zugriff (einsehen und / oder bearbeiten) auf alle Gruppen hat, die dieser administrieren soll.

Sie können die Option *Gruppenrechte für Security Officer setzen, die Gruppen oder Benutzer verwalten* dürfen im Register **Andere Einstellungen** des Knotens **Zentrale Einstellungen** einstellen.

9. Klicken Sie auf die Schaltfläche **Fertigstellen**.

Der neu angelegte Security Officer wird in der *u.trust LAN Crypt* Admin-Konsole angezeigt.

3.8.1 Zuweisen/bearbeiten der globalen Rechte

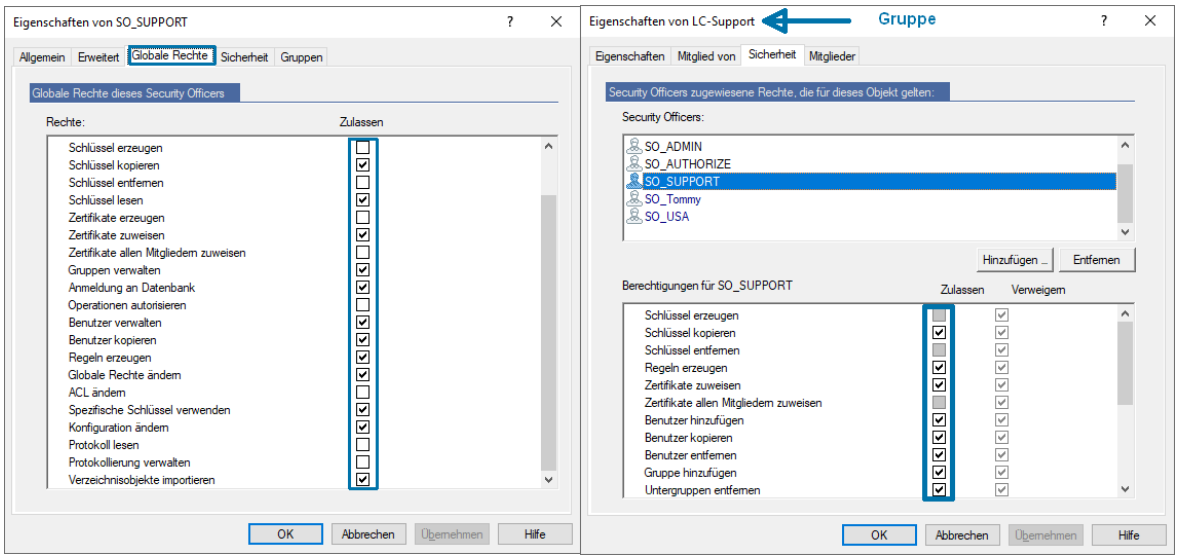
Der Security Officer muss mit globalen Rechten ausgestattet sein. Ist in der Admin-Konsole der Knoten **Security Officer Administration** markiert, werden im rechten Konsolenfenster alle vorhandenen Security Officer angezeigt. Ein Doppelklick auf einen Security Officer öffnet ein Register, über das Sie die Eigenschaften und Rechte des Security Officers anzeigen und bearbeiten können.

Über das Register **Globale Rechte** erhält der Security Officer seine „Basisrechte“ für die Administration von *u.trust LAN Crypt*. Wurde dem Security Officer bereits als man ihn anlegte, die erforderliche Berechtigung zum Ausführen bestimmter Aktionen erteilt, sind für ihn alle dazu notwendigen globalen Rechte schon aktiviert.

Hinweis: Beachten Sie, dass ein Security Officer analog zu dem ihm jeweils erteiltem globalen Recht, auch das hierfür erforderliche Gruppenrecht erhalten muss, um eine bestimmte Aktion ausführen zu können (vgl. Abschnitt 3.11.3 „*Dem Security Officer Rechte zur Bearbeitung der Gruppen zuweisen*“ auf Seite 121.

Beispiel:

Damit ein Security Officer Gruppen und Benutzer z. B. aus Verzeichnisdiensten importieren kann, muss er zusätzlich zu den globalen Rechten „*Verzeichnisobjekte importieren*“, „*Gruppen verwalten*“ und „*Benutzer verwalten*“ auch die Gruppenrechte „*Gruppe hinzufügen*“ sowie „*Benutzer hinzufügen*“ besitzen.



Hinweis: Ein Master Security Officer ist immer mit allen globalen Rechten ausgestattet.

Ein Security Officer kann global mit folgenden Rechten ausgestattet werden:

Hinweis: Durch einen Klick auf die Spaltenüberschrift **Zulassen** können alle Rechte ausgewählt werden. Ein weiterer Klick auf die Spaltenüberschrift hebt die Auswahl wieder auf.

Rechte	Beschreibung
Security Officer anlegen	Der Security Officer hat das Recht, weitere Security Officer zu erzeugen.
Profile erzeugen	Der Security Officer hat die globale Berechtigung, den Profile Resolver zu starten und Profildateien für einzelne Benutzer zu erzeugen. Dieses globale Recht ist die Voraussetzung dafür, dass die Berechtigung „*Profile erzeugen*“ für eine spezifische Gruppe bei einem Security Officer gesetzt werden kann. Das globale Recht „*Profile erzeugen*“ berechtigt den Security Officer zum Erstellen von Benutzerprofilen, wenn der Security Officer die Berechtigung „*Profile erzeugen*“ für die übergeordnete Gruppe von Benutzern hat *(siehe „Übergeordnete Gruppe eines Benutzers“ auf Seite 118).* Diese Berechtigung ist eine Voraussetzung für das Zuweisen von Werten zu Schlüsseln. Ein Security Officer, der nur das globale Recht „*Schlüssel erzeugen*“ hat, kann nur Schlüssel ohne Werte erzeugen!
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass das Recht „*Profile erzeugen*“ gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung „*Profile für alle Mitglieder erzeugen*“ für eine spezifische Gruppe gesetzt werden kann. „*Profile für alle Mitglieder erzeugen*“ berechtigt einen Security Officer zum Erzeugen von Profilen für alle Benutzer, wenn der Security Officer die Berechtigung *Profile erzeugen* für die übergeordnete Gruppe des Benutzers oder die Berechtigung *Profile für alle Mitglieder erzeugen* für eine der Gruppen, zu denen der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung „*Profile erzeugen“* eine Voraussetzung ist, um Profile für alle Mitglieder zu erzeugen, gilt daher: Wenn Sie die Berechtigung „*Profile erzeugen“* deaktivieren, wird auch die Berechtigung „*Profile für alle Mitglieder erzeugen“* deaktiviert. Wenn Sie die Berechtigung „*Profile für alle Mitglieder erzeugen“* aktivieren, wird automatisch auch die Berechtigung „*Profile erzeugen“* aktiviert.

Rechte	Beschreibung
Schlüssel erzeugen	Der Security Officer darf Schlüssel in den einzelnen Gruppen erzeugen. Das Recht „*Schlüssel erzeugen*“ alleine erlaubt dem Security Officer nur das Erzeugen von Schlüsseln ohne Wert! In der Administration können Schlüssel ohne Wert Verschlüsselungsregeln zugeordnet werden. Der Wert selbst wird erst generiert, wenn der Profile Resolver gestartet wird. Um direkt beim manuellen Anlegen auch den zum Schlüssel gehörenden Wert erzeugen zu können, benötigt der Security Officer das Recht „*Profile erzeugen“.*
Schlüssel kopieren	Der Security Officer darf Schlüssel kopieren.
Schlüssel entfernen	Der Security Officer darf Schlüssel aus den Gruppen entfernen.
Schlüssel lesen	Der Security Officer darf die Daten zu den einzelnen Schlüsseln der Gruppe sehen.
Zertifikate erzeugen	Der Security Officer darf Zertifikate für die Benutzer erzeugen.
Zertifikate zuweisen	Der Security Officer darf den Benutzern Zertifikate zuweisen. Der Security Officer darf den Assistenten zur Zertifikats-zuweisung starten. Dieses globale Recht ist die Voraussetzung dafür, dass die Berechtigung „*Zertifikate zuweisen*“ für eine spezifische Gruppe für einen Security Officer gesetzt werden kann. Zertifikate zuweisen berechtigt den Security Officer zum Zuweisen von Zertifikaten an Benutzer, wenn der Security Officer die Berechtigung „*Zertifikate zuweisen*“ für die übergeordnete Gruppe des Benutzers hat (siehe „*Übergeordnete Gruppe eines Benutzers*“ auf Seite 118).

Rechte	Beschreibung
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Zertifikate zuweisen gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Zertifikate allen Mitgliedern zuweisen für eine spezifische Gruppe gesetzt werden kann. Zertifikate allen Mitgliedern zuweisen berechtigt einen Security Officer zum Zuweisen von Zertifikaten zu Benutzern, wenn der Security Officer die Berechtigung Zertifikate zuweisen für die übergeordnete Gruppe des Benutzers oder die Berechtigung Zertifikate allen Mitgliedern zuweisen für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da das globale Recht „*Zertifikate zuweisen*“ eine Voraussetzung für „*Zertifikate allen Mitgliedern zuweisen*“ ist, gilt: Wenn Sie dieses globale Recht deaktivieren, wird auch die Berechtigung „*Zertifikate allen Mitgliedern zuweisen*“ deaktiviert. Wenn Sie das globale Recht „*Zertifikate allen Mitgliedern*“ zuweisen aktivieren, wird automatisch auch das globale Recht „*Zertifikate zuweisen*“ aktiviert.
Gruppen verwalten	Der Security Officer darf Änderungen in den Gruppen vornehmen. D. h. Untergruppen aufnehmen, Gruppen verschieben, Gruppen synchronisieren, Gruppen löschen.
Anmeldung an Datenbank	Der Security Officer darf sich an der *u.trust LAN Crypt* Datenbank anmelden. Dieses Recht ist standardmäßig immer aktiviert. Dieses Recht stellt eine Möglichkeit dar, einem Security Officer ohne großen Aufwand die Möglichkeit zu nehmen, an der *u.trust LAN Crypt*-Datenbank Veränderungen vorzunehmen (z. B., wenn er die Abteilung wechselt). Personen, die ausschließlich „Vier-Augen-Aktionen“ autorisieren dürfen, kann dieses Recht verweigert werden. Damit ist sichergestellt, dass sie neben der Autorisierung von „Vier-Augen-Aktionen“, keine Möglichkeit haben, Änderungen in *u.trust LAN Crypt* vorzunehmen.
Operationen autorisieren	Der Security Officer darf an „Vier-Augen-Aktionen“ teilnehmen.
Benutzer verwalten	Der Security Officer darf Benutzer in eine Gruppe aufnehmen / entfernen und Gruppen synchronisieren.

Rechte	Beschreibung
Benutzer kopieren	Der Security Officer darf Benutzer zu Gruppen hinzufügen (kopieren). Dieses globale Recht ist eine Voraussetzung für das Setzen der Berechtigung „*Benutzer kopieren*“ für eine spezifische Gruppe für einen Security Officer. Um einen Benutzer zu einer Gruppe hinzuzufügen, muss der Security Officer die Berechtigung „*Benutzer kopieren*“ für die übergeordnete Gruppe des Benutzers haben.
Regeln erzeugen	Der Security Officer darf Verschlüsselungsregeln erzeugen.
Globale Rechte ändern	Der Security Officer darf die globalen Rechte eines anderen Security Officers ändern.
ACL ändern	Der Security Officer darf die ACL einer Gruppe ändern.
Spezifische Schlüssel verwenden	Der Security Officer darf auch spezifische Schlüssel in Verschlüsselungsregeln verwenden und sich diese über den Knoten **Alle u.trust LAN Crypt Schlüssel** anzeigen lassen.
Konfiguration ändern	Der Security Officer darf die Konfiguration (die Pfade) ändern. Dieses Recht ist die Voraussetzung dafür, dass das Register **Konfiguration** im Knoten **Zentrale Einstellungen** angezeigt wird und das Register **Verzeichnisse** bearbeitbar ist, wenn dieser Security Officer an die Datenbank angemeldet ist.
Protokoll lesen	Für den Security Officer sind die Einstellungen für die Protokollierung und die Einträge und die Protokolleinträge sichtbar.
Protokollierung verwalten	Der Security Officer darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.
Verzeichnisobjekte importieren	Der Security Officer darf OUs, Gruppen und Benutzer aus einem Verzeichnisdienst importieren und in die *u.trust LAN Crypt*-Datenbank übertragen. Dieses globale Recht bedingt, dass der Security Officer die globalen Rechte „*Gruppen verwalten*“ und „*Benutzer verwalten*“ besitzt. Diese werden automatisch gesetzt, wenn das globale Recht „*Verzeichnisobjekte importieren*“ ausgewählt wird. Besitzt ein Security Officer dieses Recht nicht, ist der Knoten **Verzeichnis-Objekte**, der das Importieren von OUs, Gruppen und Benutzern ermöglicht, in der Administration nicht sichtbar.

Bitte beachten Sie bei der Vergabe der *globalen Rechte* folgende Punkte:

- Wird einem Security Officer ein globales Recht nicht ausdrücklich gegeben, ist er nicht mit diesem ausgestattet.
- Ein Security Officer darf in weiterer Folge nur jene Rechte ändern, die er selbst besitzt.
- Ein Security Officer darf eine ACL, die seine eigenen Rechte beschreibt, nicht ändern.
- Manche Rechte bedingen das Setzen eines zweiten Rechts. Dies wird bei der Auswahl eines solchen Rechts automatisch gesetzt.
- *u.trust LAN Crypt* kann so konfiguriert werden, dass automatisch eine ACL mit Leserechten für die Stammgruppe für einen neu erstellten Security Officer angelegt wird. Hier ist erforderlich, dass der Security Officer das globale Recht *Gruppen verwalten* oder *Benutzer verwalten* besitzt. Dadurch wird garantiert, dass der Security Officer Zugriff (einsehen und / oder bearbeiten) auf die Gruppen hat, für die er verantwortlich ist.

  Dieses Verhalten muss im Register **Andere Einstellungen** unter dem Knoten **Zentrale Einstellungen** aktiviert werden.
- Wenn ein Security Officer durch Änderung das globale Recht *Gruppen verwalten* oder *Benutzer verwalten* erhält und er keine ACL für die Stammgruppe besitzt, so wird diese angelegt. Die ACL hat Leserechte für die Gruppe. Vorhandene ACLs bleiben dabei unverändert.

Markieren Sie die *globalen Rechte*, über die der Security Officer verfügen soll, und klicken Sie auf die Schaltfläche **Übernehmen**.

Durch Klicken auf **OK** schließen Sie den Dialog.

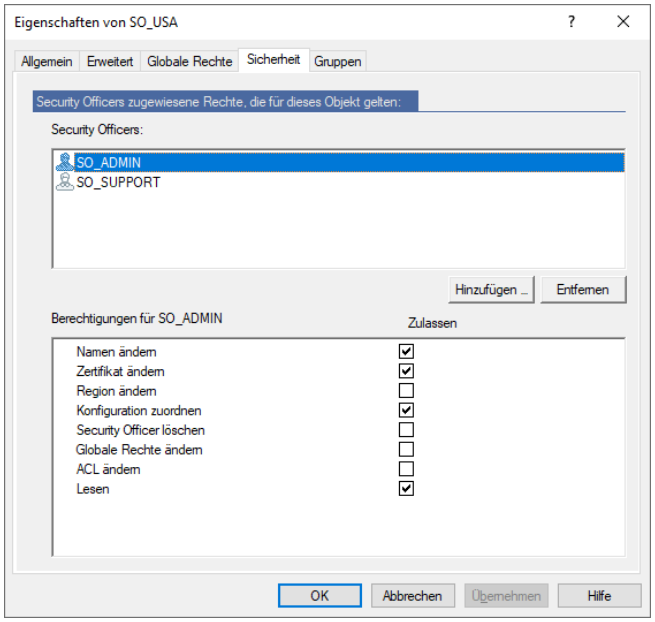
3.8.2 Rechte zum Bearbeiten der Einstellungen für einen Security Officer

Anderen Security Officers können Rechte zum Bearbeiten der Einstellungen für einen Security Officer übertragen werden. Einem Security Officer muss ein solches Recht durch einen Master Security Officer zunächst einmal explizit erteilt werden. Zudem ist zu beachten, dass Security Officer nicht die Einstellungen eines Master Security Officers ändern kann. Ein Master Security Officer besitzt immer alle Rechte.

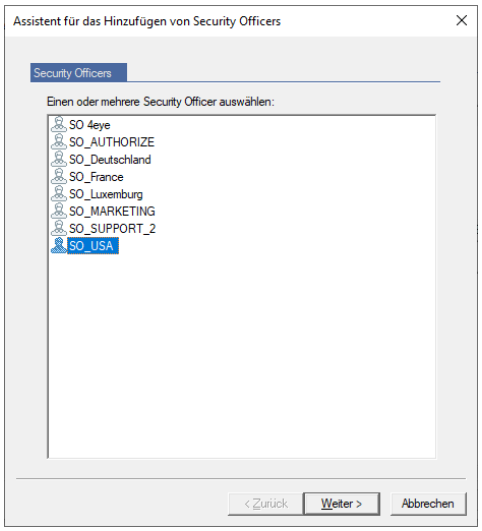
Hinweis: Ein Master Security Officer ist immer imstande, solche Einstellungen wieder zu ändern.

Welche Einstellungen ein Security Officer für einen anderen Security Officer ändern darf, ist grundsätzlich zunächst einmal davon abhängig, welche globalen Rechte, dieser selbst besitzt. So können zudem ggf. auch mehrere Berechtigungen erforderlich sein, um eine bestimmte Funktion ausüben zu dürfen. Soll beispielsweise ein Security Officer das Recht erhalten, einen anderen Security Officer löschen zu dürfen, muss dieser Security Officer die globalen Rechte *ACL ändern* und *Security Officer erzeugen* besitzen.

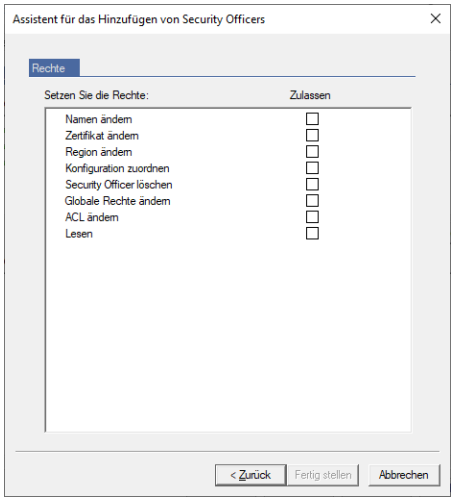
Im Register **Sicherheit** können Sie festlegen, welche Rechte andere Security Officer bezogen auf dieses Objekt (= Security Officer) besitzen. Im oberen Teil des Dialogs werden jene Security Officer angezeigt, die das Recht besitzen, die Einstellungen für diesen Security Officer zu bearbeiten.



1. Durch Klicken auf **Hinzufügen ...** wird ein Assistent zum Hinzufügen eines Security Officers gestartet. Auf der ersten Seite des Assistenten wird aus der Liste der vorhandenen Security Officer der gewünschte ausgewählt.



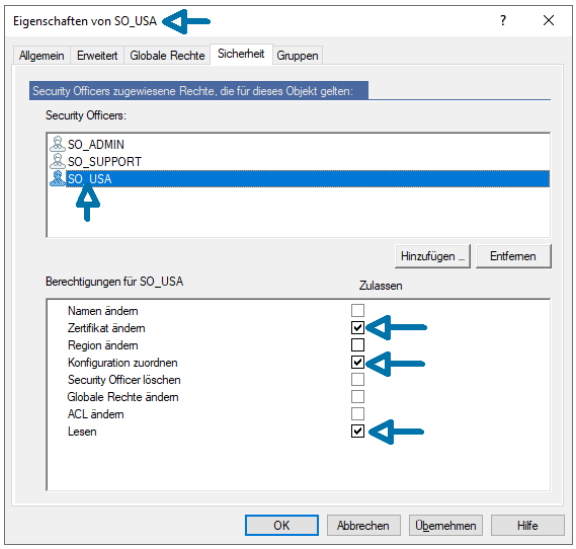
2. Klicken auf **Weiter** öffnet einen Dialog, auf der die Rechte für diesen Security Officer, betreffend die Bearbeitungsrechte für dieses Objekt (den Security Officer, dessen Eigenschaften derzeit bearbeitet werden), eingestellt werden können.



Hinweis: Durch einen Klick auf die Spaltenüberschrift **Zulassen** können alle Rechte ausgewählt werden. Ein weiterer Klick auf diese Spaltenüberschrift hebt die Auswahl aller Rechte wieder auf. Ausgegraute Rechte können dem Security Officer (SO) aufgrund der Einstellungen in den globalen Rechten nicht zugestanden werden (siehe "*Zuweisen / bearbeiten der globalen Rechte*" auf Seite 91).

Rechte	Beschreibung
Namen ändern	Der Security Officer erhält das Recht, den Namen dieses Security Officers ändern zu dürfen.
Zertifikat ändern	Der Security Officer erhält das Recht, das Zertifikat dieses Security Officers ändern zu dürfen.
Region ändern	Der Security Officer erhält das Recht, die Zuweisung der Region dieses Security Officers ändern zu dürfen.
Konfiguration zuordnen	Der Security Officer erhält das Recht, die Konfiguration (bearbeiten und zuordnen der Pfade) dieses Security Officers ändern zu dürfen.
Security Officer löschen	Der Security Officer erhält das Recht, diesen Security Officer löschen zu dürfen.
Globale Rechte ändern	Der Security Officer erhält das Recht, die Einstellungen für die globalen Rechte dieses Security Officers ändern zu dürfen.
ACL ändern	Der hinzugefügte Security Officer erhält das Recht, die ACL dieses Security Officers ändern zu dürfen.
Lesen	Der Security Officer erhält das Recht, sich diesen Security Officer anzeigen zu lassen. Dieser wird ihm dann nach seiner Anmeldung an der *u.trust LAN Crypt* Admin-Konsole unter dem Knoten **Zentrale Einstellungen/Security Officer Administration** angezeigt. Wenn dieses Recht nicht erteilt wurde, können auch alle weiteren Rechte, die eine Bearbeitung von Security Officer durch einen anderen Security Officer ermöglichen, nicht ausgeführt werden. Dieses Recht wird aus diesem Grund automatisch erteilt, sobald einem Security Officer irgendein Recht zum Bearbeiten der Einstellungen eines anderen Security Officers übertragen wurde.

Die Rechte **Zertifikat ändern**, **Konfiguration zuordnen** und **Lesen** können auch dem Security Officer gegeben werden, dessen Eigenschaften hier definiert werden. Dazu muss er selbst in die Liste der Security Officer, die Rechte auf dieses Objekt haben (in diesem Fall er selbst), aufgenommen werden.



Zertifikat ändern

Voraussetzung dafür ist das Recht **Lesen**. Es erlaubt dem Security Officer, sein eigenes Zertifikat zu ändern.

Konfiguration zuordnen

Ermöglicht dem Security Officer, sich selbst eine andere Konfiguration zuzuordnen.

Lesen

Zeigt den im Knoten **Zentrale Einstellungen \ Security Officer Administration** angelegten Security Officer an. Für den Security Officer sind die für ihn gesetzten Rechte sichtbar.

Hinweis: Rechte, für die das Kontrollkästchen ausgegraut ist, können nicht vergeben werden, da der ausgewählte Security Officer selbst nicht über die globalen Rechte verfügt, die dafür notwendig sind.

3. Statten Sie den Security Officer durch Anklicken der Kontrollkästchen mit den entsprechenden Rechten aus und klicken Sie auf **Übernehmen.**

   Der Security Officer wird jetzt im oberen Teil des Registers **Sicherheit** angezeigt. Im unteren Teil des Registers zeigt eine ACL die expliziten Berechtigungen dieses Security Officers für das Bearbeiten der Einstellungen des aktuell gewählten Security Officers an.

3.8.3 Alle Rechte für Gruppen/OUs eines spezifischen Security Officer

Um die Rechte eines spezifischen Security Officer für alle Gruppen / OUs einzusehen, für die der Security Officer Berechtigungen hat, doppelklicken Sie im Knoten **Security Officer Administration** auf den entsprechenden Security Officer.

Klicken Sie im Eigenschaftendialog des Security Officers auf den Reiter **Gruppen**. Der dann angezeigte Dialog zeigt zwei Listenansichten:

- Die obere Listenansicht zeigt alle Gruppen / OUs, für die dieser Security Officer Berechtigungen hat.
- Die zweite Listenansicht *Rechte auf …* zeigt die entsprechenden Rechte des Security Officers für die ausgewählte Gruppe / OU.

Sie erhalten so auf einfache Weise einen Überblick zu allen Rechten, die ein spezifischer Security Officer für die verschiedenen Gruppen in Ihrer Organisationsstruktur hat.

Hinweis: Sie können die Rechte eines Security Officers in dieser Ansicht nicht ändern. Dies ist nur im Eigenschaftendialog einer Gruppe möglich.

Hinweis: Für jede in der oberen Listenansicht aufgeführte Gruppe können die Berechtigungen des Security Officers angezeigt werden (jeweils dargestellt durch ein Häkchen bei Zulassen oder Verweigern). Gruppen, für die ein Security Officer Rechte geerbt hat, werden an dieser Stelle nicht angezeigt.

3.8.4 Wechsel oder Erneuern eines MSO- oder Security Officer-Zertifikats

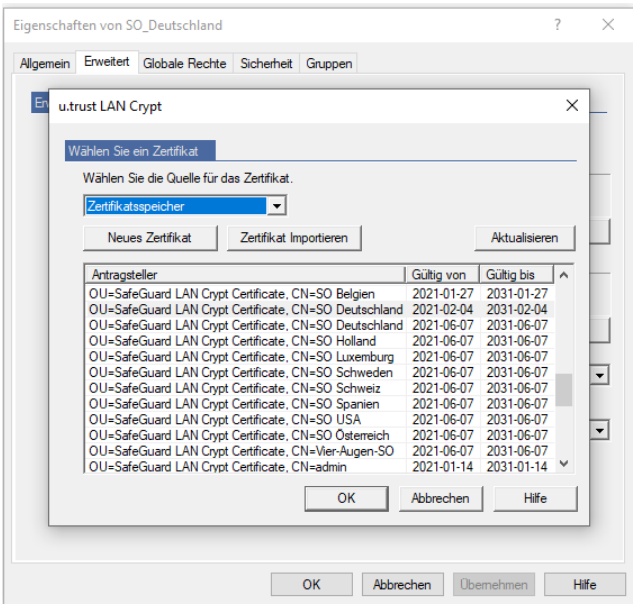
Für den Wechsel bzw. die Erneuerung eines (M)SO-Zertifikats gibt es folgende Möglichkeiten:

Variante 1: Über die Security Officer Administration

1. Starten Sie die *u.trust LAN Crypt* Admin-Konsole und melden Sie sich dort als Master Security Officer an. Alternativ können Sie sich auch als Security Officer anmelden, der das Recht hat, das Zertifikat des betroffenen Security Officers zu ändern. Dies kann auch der betroffene Security Officer selbst sein, sofern er über das benötigte Recht verfügt und sein Zertifikat noch gültig ist.
2. Wechseln Sie zum Knoten **Zentrale Einstellungen** und von dort in den Knoten **Security Officer Administration**.
3. Klicken Sie im Fenster rechts mit der rechten Maustaste auf den betroffenen Security Officer, und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
4. Wechseln Sie zum Register **Erweitert**.

5. Klicken Sie im Abschnitt *Verschlüsselungszertifikat* auf die Schaltfläche **Suchen**, um ein neues Verschlüsselungszertifikat für den Security Officer auszuwählen.

6. Klicken Sie gegebenenfalls im Abschnitt *Signaturzertifikat (optional)* auf die Schaltfläche ***Suchen***, um ein neues Signaturzertifikat für den Security Officer auszuwählen.

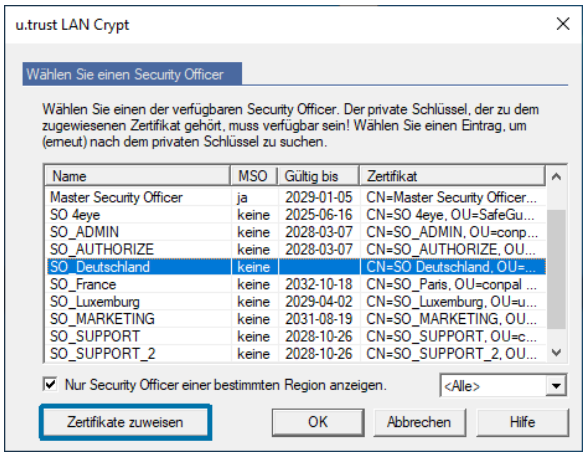


7. Wählen Sie das gewünschte Zertifikat aus, oder wählen bzw. erstellen Sie ein neues Zertifikat. Sie können alternativ auch ein vorhandenes Zertifikat importieren. Wenn Sie das Zertifikat für den Security Officer gewählt haben, klicken Sie auf **OK**.

Hinweis: Security Officer-Signaturzertifikate lassen sich nur per Variante 1 ändern und nicht per Variante 2.

Variante 2: Über den Wiederherstellungsschlüssel

1. Starten Sie die *u.trust LAN Crypt* Admin-Konsole.
2. Markieren Sie im Dialogfenster zur Auswahl des Security Officers den betroffenen (M)SO.
3. Klicken Sie auf die Schaltfläche **Zertifikate zuweisen** und folgen Sie den Anweisungen des *Assistenten für Wiederherstellungsschlüssel*.



Im Normalfall sollten Sie mit Variante 1 arbeiten. Variante 2 ist primär dazu vorgesehen, einen alternativen Weg zu haben, falls sich kein Security Officer mit ausreichenden Rechten mehr an die *u.trust LAN Crypt* Admin-Konsole anmelden kann.

Hinweis: Voraussetzung für „Variante 2“ ist das Vorhandensein eines Wiederherstellungsschlüssels. Beachten Sie in dem Fall, dass die hierfür erforderlichen Teilschlüssel eingegeben werden müssen.

Unabhängig von der verwendeten Methode stellen Sie sicher, dass dann auch die Profildateien aller Benutzer, die von dem betroffenen Security Officers administriert werden, neu erzeugt werden müssen. Geschieht dies nicht, hat das zur Folge, dass wegen der Erneuerung des Security Officer-Zertifikats (**.cer*) die Profildateien von den betroffenen Clients nicht mehr geladen werden können.

Es ist möglich, die Zuweisung von Zertifikaten nur mit *zusätzlicher Autorisierung* zu erlauben. Eine derartige Einstellung wirkt sich auch beim Wechsel des Security Officer-Zertifikats aus.

3.9 Anmeldung an der Administration

Um sich an der Administration von *u.trust LAN Crypt* (Admin-Konsole) anmelden zu können, muss ein Security Officer mit dem Recht zur Anmeldung ausgestattet sein. Master Security Officer haben dieses Recht immer, da sie automatisch mit allen zur Verfügung stehenden Rechten ausgestattet sind.

Nach Aufruf der Administration im Startmenü unter **u.trust LAN Crypt Administration** oder über den Pfad:

```
c:\Programme (x86)\utimaco\u.trust LAN Crypt\Administration\SGLCAdmin.msc
```

wird für den (Master) Security Officer der Anmeldedialog von *u.trust LAN Crypt* angezeigt.

Alle berechtigten Security Officer werden in der Liste angezeigt. Durch Aktivieren der Option **Nur Security Officer einer bestimmten Region anzeigen** und der Auswahl der entsprechenden Region, kann die Anzeige auf die Security Officer dieser Region eingeschränkt werden. Security Officer, die keiner Region zugeordnet sind, und auch Master Security Officer werden dann ebenfalls mit angezeigt.

Damit eine Anmeldung möglich ist, muss auf den zum Zertifikat gehörenden privaten Schlüssel (Software-Schlüssel oder auf einem Token / einer Smartcard) zugegriffen werden können.

Nach der Auswahl des gewünschten Security Officers und dem Klicken auf **OK** wird die Administration von *u.trust LAN Crypt* geöffnet.

Wiederherstellungsschlüssel

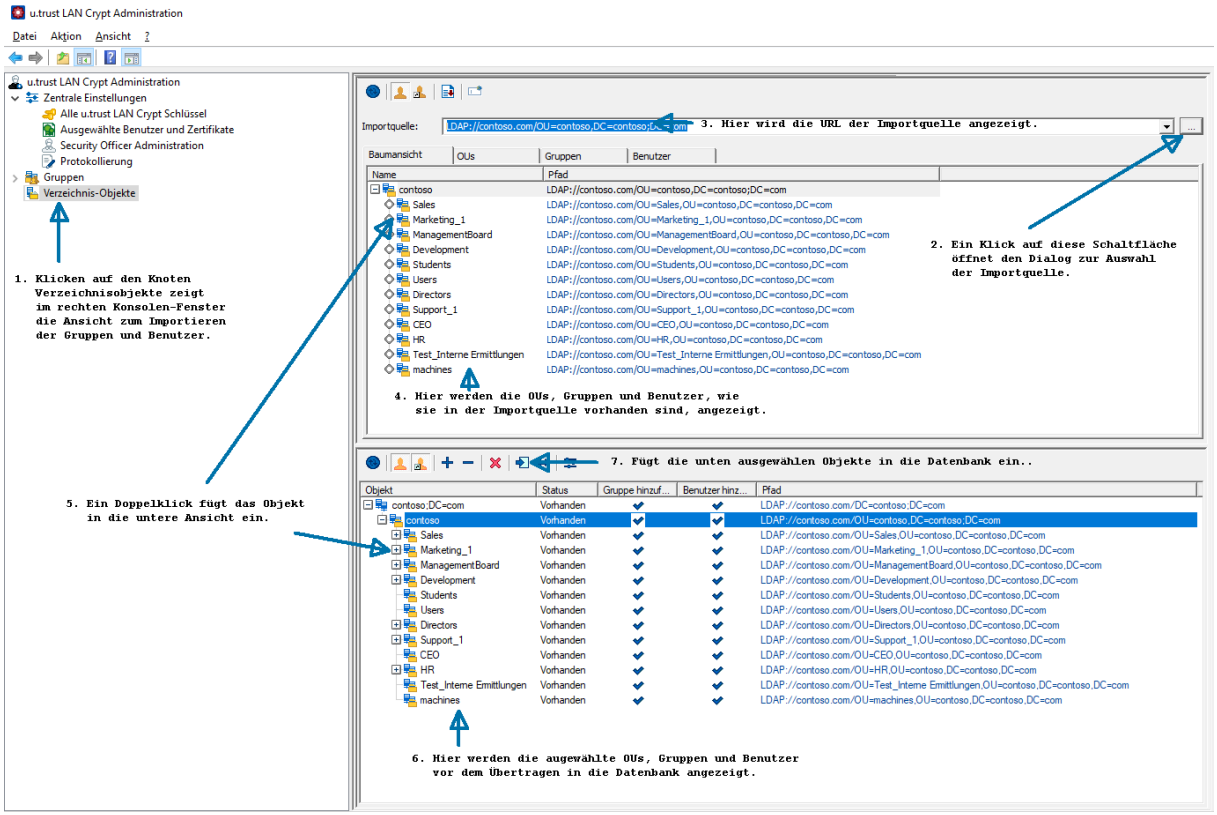
Ist der zum Zertifikat gehörende Schlüssel eines Security Officers abgelaufen, beschädigt oder verloren gegangen, besteht die Möglichkeit, das Zertifikat durch die Eingabe eines Wiederherstellungsschlüssels zu erneuern (siehe Abschnitt 3.5.10 „*Wiederherstellungsschlüssel*“ auf Seite 74).

Hinweis: Wird während des Wiederherstellens ein neues Zertifikat erzeugt, so wird dieses Zertifikat mit zugehörigem Passwort (*.p12*) unter dem konfigurierten Pfad gespeichert.

3.10 Gruppen und Benutzer importieren

u.trust LAN Crypt ermöglicht den Import von Gruppen und Benutzern aus Verzeichnisdiensten, auf die über LDAP oder aus der Domäne oder auch über den Import aus einer manuell erstellten Datei, die die Gruppen und Benutzer mit den jeweiligen Zugehörigkeiten enthält, zugegriffen werden kann.

Wenn Sie auf den Knoten **Verzeichnis-Objekte** klicken, werden im rechten Konsolenfenster die Dialoge zum Import und zur Zusammenstellung der Gruppen für den Import in die *u.trust LAN Crypt*-Datenbank angezeigt.



Hinweis: Ist der Knoten **Verzeichnis-Objekte** nicht sichtbar, verfügt der angemeldete Security Officer nicht über das globale Recht *Verzeichnisobjekte importieren*. Erst wenn ihm dieses globale Recht gegeben wird, wird der Knoten **Verzeichnis-Objekte** angezeigt.

Hinweis: Verwenden Sie aus Gründen der Performance beim Aufruf der Importquelle über LDAP immer den FQDN (Fully Qualified Domain Name).

3.10.1 Benutzer und Benutzergruppen aus einer Datei importieren

Benutzer und Benutzergruppen können auch aus einer Datei importiert werden. Die importierten Benutzer und Gruppen werden in der *u.trust LAN Crypt* Administration angelegt und unter den Knoten **Gruppen** und **Verzeichnis-Objekte** angezeigt.

Zum Importieren von Benutzern und Gruppen aus einer Datei wählen Sie im Dialog *Importquelle* **Datei suchen** aus. Durch Klicken auf die Schaltfläche **Durchsuchen** können Sie

anschließend die Datei auswählen, aus der die Benutzer und Gruppen importiert werden sollen (siehe „*Importquelle auswählen*“ auf Seite 109).

Bei der Importdatei handelt es sich um eine Textdatei mit einer beliebigen Endung (als Standardendung wird „*.lcg*“ vorgeschlagen). Der Inhalt der Datei muss ein bestimmtes Format aufweisen.

Das Format der Importdatei

Eine Importdatei enthält mehrere Abschnitte. Die einzelnen Abschnitte können durch eine beliebige Anzahl von Leerzeilen getrennt sein.

Jeder Abschnitt steht für je einen Benutzer bzw. je eine Gruppe.

Jeder Abschnitt besteht aus einer Kopfzeile und einer bestimmten Anzahl von Zeilen mit je einem Schlüsselwort. Zeilen müssen durch ein Zeilenumbruch-Zeichen abgeschlossen werden. Zwischen den Zeilen eines Abschnitts dürfen keine Leerzeilen vorkommen.

Die Kopfzeile wird in eckige Klammern gesetzt und enthält den Abschnittnamen. Der Abschnittname wird verwendet, um die Mitgliedschaften von Benutzern und Gruppen zu definieren.

Die Schlüsselwörter geben die Daten der Benutzer und Gruppen an. Diese Daten werden auch in den *Eigenschaften*-Dialogen der Gruppen und Benutzer angezeigt.

Schlüsselwörter	Beschreibung
type=	USER GROUP Gibt an, ob es sich bei dem importierten Objekt um einen Benutzer (USER) oder um eine Gruppe (GROUP) handelt.
name=	Gibt den Anmeldenamen des Benutzers an. Wird in der *u.trust LAN Crypt*-Administration als *Logonname* angezeigt.
display= optional	Ermöglicht die Angabe eines Benutzernamens, der nicht identisch mit dem Anmeldenamen ist. Wird in der *u.trust LAN Crypt*-Administration als *Benutzername* angezeigt. Ist hier kein Name eingetragen, so wird der unter name= eingegebene Anmeldename als *Benutzername* in der *u.trust LAN Crypt* Administrations-Konsole angezeigt.
mail= optional	Ermöglicht die Angabe der E-Mail-Adresse des Benutzers. Diese wird unter Details in den Benutzereigenschaften angezeigt. **Hinweis:** Die E-Mail-Adresse wird auch in die Passwort-protokolldatei für von *u.trust LAN Crypt* erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN-Mailers via E-Mail verwendet werden.

Schlüsselwörter	Beschreibung
members=	Gibt für Gruppen an, welche Benutzer und andere Gruppen, Mitglied sind. Um ein Mitglied hinzuzufügen, geben Sie den Namen der Kopfzeile des Abschnitts, der den Benutzer bzw. die Gruppe beschreibt, ein (z. B. U_RLU,G_PDM). Die einzelnen Mitglieder der Gruppe müssen durch Kommas getrennt werden.

Hinweis: Durch die Verwendung von // am Zeilenbeginn kann an jeder beliebigen Stelle der Datei ein Kommentar eingefügt werden.

Hinweis: Zwischen Groß- und Kleinschreibung wird in der Importdatei NICHT unterschieden.

Beispiel:

```
[U_UF]
type=USER
name=UF
Display=Ulrike Falke
Mail=Ulrike.falke@contoso.com
// Mein Kommentar ...
[U_PW]
type=USER
name=PW
Mail=pw@contoso.com
[U_JG]
type=USER
name=JG
[U_RLU]
type=USER
name=RLU
[G_COMPANY]
type=GROUP
name=Company members=G_QA, G_GF, G_NI, G_FFM, U_RLU, U_RK
// Mein Kommentar ... ...
[G_QA] type=GROUP name=QA members=U_UF, U_KS, U_PW
[G_PDM] type=GROUP name=PDM members=U_RLU
```

3.10.2 Symbole

 Aktualisiert die Ansicht im jeweiligen Fenster.

 Zeigt die Benutzer in den jeweiligen Gruppen an.

 Zeigt auch die Mitgliedschaften von Gruppen und Benutzern in den jeweiligen Gruppen an.

Mitgliedschaften, bei denen das Objekt nicht direkt in der Gruppe enthalten ist, werden grau dargestellt.

 Fügt das ausgewählte Objekt in die untere Ansicht ein. Entspricht einem Doppelklick auf das ausgewählte Objekt.

 Als neuer Pfad übernehmen.

Erlaubt es, die Anzeige der Struktur einzuschränken. Wird ein Knoten markiert und anschließend auf diese Schaltfläche geklickt, wird nur noch die Struktur unter dem markierten Knoten angezeigt. Der Pfad wird zusätzlich der Drop-Down-Liste hinzugefügt, sodass wieder schnell zu dieser Anzeige gewechselt werden kann.

 Zeigt die Baumstruktur an

 Schließt die Baumstruktur.

 Löscht ein markiertes Objekt aus der Ansicht.

 Fügt die im rechten unteren Fenster angezeigten Objekte in die *u.trust LAN Crypt* Datenbank ein.

 Synchronisiert die im rechten unteren Fenster angezeigten Objekte mit den bereits in der Datenbank vorhandenen.

 Öffnet den Dialog zum Festlegen der Übernahmeoptionen.

Die Übernahmeoptionen müssen vor der Übernahme aus der Importquelle festgelegt werden.

3.10.3 Importquelle auswählen

Die URL des Servers, von dem die Daten importiert werden sollen, kann direkt in das Eingabefeld *Importquelle* eingegeben werden (z. B. `LDAP://usw-ni/dc=usw-ni,dc=u.trust,dc=de` für den Active Directory Verzeichnisdienst auf dem Domänen-Controller `usw-ni`).

Wenn Sie auf die Schaltfläche **Durchsuchen** klicken, stellt *u.trust LAN Crypt* einen Dialog zur Auswahl der Importquelle zur Verfügung:

LDAP://

- **Domäne**

  Ist der Rechner Mitglied in einer Active Directory Domäne, wird die gesamte Struktur der Domäne, wie sie am Domänen-Controller vorhanden ist, angezeigt.

  Hinweis: Der Import von Built-in-Gruppen aus dem Active Directory ist nicht möglich. Es wird daher empfohlen, die Benutzer in OUs bzw. Gruppen zu organisieren und diese zu importieren.

- **Container suchen**

  Ist der Rechner Mitglied in einer Active Directory-Domäne, wird nach dem Klicken auf die Schaltfläche **Durchsuchen** (diese wird angezeigt, nachdem *Container suchen* markiert wurde) ein weiterer Dialog angezeigt. In diesem Dialog kann dann ein bestimmter Knoten in der Active Directory-Struktur ausgewählt werden.

WinNT://

- **Computer**

  Zeigt die lokalen Gruppen und Benutzer des Rechners an, an dem Sie angemeldet sind. Diese Gruppen und Benutzer werden normalerweise nur für Testzwecke verwendet.

- **Domäne**

  Ist der Rechner Mitglied in einer Windows NT-Domäne, wird die gesamte Struktur der Domäne, wie sie am Domänen-Controller vorhanden ist, angezeigt.

  Hinweis: Bei Verwendung des WinNT-Protokolls können bei einer Synchronisation umbenannte Benutzer nicht von neu angelegten unterschieden werden, da das WinNT-Protokoll Benutzerobjekten keine eindeutige GUID zuweist.

FILE://

- **Datei suchen**

  Zum Importieren von Benutzern und Gruppen aus einer Datei wählen Sie im Dialog *Importquelle* **Datei suchen** aus. Durch Klicken auf die Schaltfläche **Durchsuchen** können Sie anschließend die Datei auswählen, aus der die Benutzer und Gruppen importiert werden sollen.

Die Datei muss vor dem Import in einem bestimmten Format erstellt werden. Für Informationen zum Erstellen der Importdatei (siehe *Benutzer und Benutzergruppen aus einer Datei importieren* auf Seite 105).

Wenn Sie eine Importquelle ausgewählt haben, zeigt ein Klick auf die Schaltfläche **Übernehmen** die URL der Quelle unter *Pfad* an.

Durch Klicken auf **OK** werden die ausgewählten Daten im rechten oberen Teil der Konsole angezeigt. Diese Ansicht erlaubt die Anzeige der ausgewählten Daten in einer Baumansicht, nach OUs, Gruppen und Benutzer.

Nur für LDAP-Server

Ist der Administrationsrechner nicht Mitglied einer Domäne, können Sie die Gruppen und Benutzer folgendermaßen von einem Server importieren:

1. Geben Sie im Register **Server** im Knoten **Zentrale Einstellungen** den Namen des Servers, den Benutzernamen und das Passwort ein.

2. Wählen Sie, ob es sich für LDAP bzw. SSL um die <*Microsoft*> bzw. <*Novell*> Implementierung handelt.

   Hinweis: Der Import aus einem Novell-Verzeichnisdienst wird seit LAN Crypt Version 3.90 nicht mehr unterstützt. Auch andere Novell-Funktionalitäten werden ebenfalls nicht mehr unterstützt und sind in der Administration nicht funktionsfähig.

3. Geben Sie in das Eingabefeld *Importquelle* die Adresse des Servers ein, von dem die Daten importiert werden sollen.

3.10.4 Vorbereitung zur Übernahme in die u.trust LAN Crypt-Datenbank

Im oberen rechten Konsolenfenster werden die OUs, Gruppen und Benutzer, wie sie in der Importquelle vorhanden sind, angezeigt.

Hier können Sie auswählen, welche der angezeigten OUs, Gruppen oder Benutzer in die *u.trust LAN Crypt*-Datenbank aufgenommen werden sollen. Die ausgewählten Objekte werden in einem ersten Schritt in die darunterliegende Ansicht übernommen, in der sie noch einmal bearbeitet werden können.

Hinweis: Das Hinzufügen eines Knotens in die untere Ansicht fügt das Objekt noch nicht in die Datenbank ein. Hier werden die Objekte nur zusammengestellt. Um sie in die Datenbank zu übertragen, klicken Sie auf **In die Datenbank einfügen** oder **Synchronisieren**.

3.10.4.1 Übernahmeeinstellungen

Zur Performance-Optimierung können Übernahmeeinstellungen festgelegt werden. Diese Übernahmeeinstellungen betreffen nur die Übernahme in die untere Ansicht, zur Vorbereitung auf das Übertragen der Daten in die Datenbank.

Klicken auf das Symbol für die Übernahmeeinstellungen öffnet einen Dialog mit drei Optionen:

- **Status der Objekte in der Datenbank anzeigen**

  Wirkt sich nur aus, wenn in der Datenbank bereits Einträge vorhanden sind, also beim Synchronisieren der Datenbank. Ist diese Option ausgewählt, wird in der unteren Ansicht für jedes Objekt angezeigt:

  - Ob es bereits in der Datenbank vorhanden ist (in der Spalte *Status*).
  - Ob der angemeldete Security Officer das Recht besitzt, die Gruppen zu modifizieren (in der Spalte *Gruppe hinzufügen*). Ein rotes Kreuz besagt, dass der Security Officer kein Recht hat, die Gruppe hinzuzufügen. Ein grünes Häkchen bedeutet, dass er dieses Recht besitzt.
  - Ob der angemeldete Security Officer das Recht besitzt, Benutzer hinzuzufügen (in der Spalte *Benutzer hinzufügen*). Ein rotes Kreuz besagt, dass der Security Officer kein Recht hat, Benutzer hinzuzufügen. Ein grünes Häkchen bedeutet, dass er dieses Recht besitzt.

- **Mitgliedschaften neu berechnen und anzeigen**

  Ist diese Option aktiviert, werden auch die Gruppenmitgliedschaften (Gruppen und Benutzer, die nicht direkte Mitglieder der einzelnen Gruppen sind) angezeigt. Zur Unterscheidung zu den direkten Mitgliedern werden diese mit grauen Symbolen dargestellt.

  Hinweis: Die Berechnung der Mitgliedschaften kann auch erst beim Übernehmen in die Datenbank vorgenommen werden.

- **Sortieren**

  Da die alphabetische Sortierung der Einträge bei umfangreichen Gruppen sehr zeitintensiv werden kann, werden die Einträge standardmäßig nicht sortiert. Wenn Sie die Objekte alphabetisch sortieren möchten, wählen Sie diese Option.

Aktualisieren der Ansicht

Wurden beim Übernehmen keine Optionen gesetzt, können diese Aktionen nach der Übernahme über die Schaltfläche **Aktualisieren** ausgeführt werden. Klicken auf **Aktualisieren** öffnet einen Dialog mit denselben Optionen. Die Aktualisierung betrifft nur die Daten in der unteren Ansicht.

3.10.4.2 Übernehmen in die untere Ansicht

Durch Doppelklick auf einen Knoten bzw. durch Markieren des Knotens und Klicken auf die Schaltfläche **Übernehmen** werden die Objekte aus der Struktur der Importquelle in die untere Ansicht übertragen.

Bevor die Objekte übertragen werden, wird ein Dialog angezeigt, in dem ausgewählt werden kann, wie die einzelnen Container und Objekte übernommen werden sollen.

- **Nur dieses Objekt übernehmen**

  Fügt das ausgewählte Objekt ohne seinen Inhalt ein.

- **Direkte Mitglieder auch übernehmen**

  Fügt alle Objekte, die in dem ausgewählten Container existieren, ein.

- **Alle Mitglieder auch rekursiv übernehmen**

  Fügt alle Objekte, die in diesem Container direkt existieren, ein sowie alle Objekte, die Mitglieder sind, und in einem anderen Container existieren. Die Mitglieder werden in ihrer vollständigen Hierarchie übernommen.

Nach der Auswahl der gewünschten Option und dem Klicken auf **OK** werden die Objekte in die untere Ansicht übernommen und sind damit bereit zum Einfügen in die *u.trust LAN Crypt*-Datenbank.

Vor der Übernahme in die Datenbank können dieser Ansicht weitere Gruppen (z. B. auch aus anderen Quellen) hinzugefügt werden und dann in einem Schritt in die Datenbank eingefügt werden.

3.10.4.3 Daten in die Datenbank einfügen bzw. synchronisieren

Die Objekte werden erst in die *u.trust LAN Crypt*-Datenbank eingefügt, nachdem sie in der unteren Ansicht zusammengestellt wurden und dort dann die Schaltflächen **In die Datenbank einfügen** bzw. **Synchronisieren** gedrückt werden.

Hinweis: Werden Objekte zu einer bestehenden Struktur hinzugefügt, so müssen Sie sie immer zuerst zur Datenbank hinzufügen. Klicken Sie dazu auf **In die Datenbank einfügen**.

Synchronisieren wird verwendet, wenn sich ausschließlich die Relationen zwischen den Objekten verändert haben.

Nach dem Klicken auf **In die Datenbank einfügen**, werden die Objekte zuerst eingefügt und anschließend wird der Synchronisationsprozess gestartet. Dieser Prozess beginnt mit einem Dialog, der verschiedene Optionen bietet:

- **Komplette Datenbank synchronisieren**

  Wird diese Option gewählt, werden alle in der *u.trust LAN Crypt*-Datenbank enthaltenen Einträge mit jenen in der Importquelle synchronisiert. Änderungen werden auf einer im Anschluss folgenden Zusammenstellung angezeigt.

Diese Option muss gewählt werden, wenn Objekte im Active Directory gelöscht wurden und diese dann auch aus der Datenbank gelöscht werden sollen.

Hinweis: Die komplette Synchronisierung kann bei einer komplexen Struktur viel Zeit in Anspruch nehmen.

- **Nur sichtbare Einträge synchronisieren**

  Bezieht sich auf die Auswahl im rechten unteren Fenster der Admin-Konsole.

- **Alle Mitgliedschaften neu berechnen**

  Wird diese Option gewählt, werden alle Mitgliedschaften auf Basis der Importquelle neu berechnet und in die Datenbank eingefügt. Mitgliedschaften werden eingefügt, auch wenn sie bei der Anzeige im rechten unteren Konsolenfenster ausgeschaltet waren (die Option **Mitgliedschaften berechnen** in den Übernahmeeinstellungen war ausgeschaltet).

- **Sichtbare Mitgliedschaften verwenden**

  Wird diese Option gewählt, werden nur die im rechten unteren Konsolenfenster sichtbaren Relationen in die Datenbank eingefügt. „Ausgeblendete Mitgliedschaften“ (**Mitgliedschaften berechnen** in den Übernahmeeinstellungen deaktiviert) werden nicht in die Datenbank eingefügt.

  Hinweis: Wird diese Option beim Synchronisieren verwendet und die Mitgliedschaften wurden für in der Datenbank existierende Objekte in der rechten unteren Konsolenansicht ausgeblendet, werden zuvor vorhandene Mitgliedschaften in der Datenbank gelöscht.

Nach der Auswahl einer Option und dem Klicken auf **OK** wird ein Dialog angezeigt, der die Synchronisation dokumentiert. Die Änderungen müssen in diesem Dialog bestätigt werden.

- **Alle Einträge**

  Zeigt alle Änderungen in einer Liste an. Entspricht der Summe der Einträge auf den weiteren Seiten.

- **Gelöschte Objekte**

  Zeigt die Objekte an, die seit der letzten Synchronisation in der Importquelle (Server) gelöscht wurden, die aber in der *u.trust LAN Crypt*-Datenbank noch vorhanden sind.

- **Neue Relationen im Verzeichnis**

  Zeigt die Objekte und Mitgliedschaften an, die zur *u.trust LAN Crypt*-Datenbank hinzugefügt wurden bzw. die seit der letzten Synchronisation in der Importquelle (Server) neu angelegt und noch nicht in die Datenbank übernommen wurden.

- **Alte Relationen in der Datenbank**

  Zeigt Objekte und Mitgliedschaften an, die in der Datenbank zwar noch vorhanden sind, in der Importquelle aber nicht mehr. Beispielsweise könnten auf dem Server Gruppen gelöscht oder Mitgliedschaften geändert worden sein.

Hinweis: Bei der Synchronisation, werden nur Objekte ausgewertet, die mindestens einmal aus einer Importquelle in die Datenbank importiert wurden.

Werden in einer Importquelle Objekte gelöscht, werden diese Änderungen nur in die Datenbank übernommen, wenn die Option *Komplette Datenbank synchronisieren* verwendet wird. In der Administration manuell hinzugefügte Gruppen und Benutzer werden bei der Synchronisation nicht ausgewertet und somit auf diesen Seiten nicht angezeigt.

Die Aktion für jedes aufgelistete Objekt kann in dieser Ansicht aufgehoben werden, indem durch einen Klick das Häkchen bei der entsprechenden Aktion entfernt wird. Es werden nur die mit einem Häkchen versehenen Aktionen ausgeführt. Durch Klicken auf **OK** wird die Synchronisation der Daten abgeschlossen.

Nachdem OUs, Gruppen und Benutzer importiert wurden, können den einzelnen Organisationseinheiten bzw. Regionen die verantwortlichen Security Officer zugeordnet werden.

3.10.4.4 Gruppen manuell einfügen

Zum manuellen Erzeugen von Gruppen markieren Sie den Knoten/die Gruppe, unter dem/der Sie eine neue Gruppe anlegen wollen und klicken Sie auf **Neue Gruppe** im Kontextmenü.

Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **OK**. Die Gruppe wird nun in der *u.trust LAN Crypt*-Administration angezeigt.

Über den *Eigenschaften*-Dialog der Gruppe können Sie der Gruppe existierende Benutzer hinzufügen bzw. neue Benutzer erzeugen.

Im Gegensatz zu importierten Gruppen können manuell erzeugte Gruppen via „*Drag & Drop*“ auch in der Hierarchie verschoben werden.

3.10.4.5 Verknüpfungen zwischen Gruppen

Um Verknüpfungen zu Gruppen herzustellen, können einzelne Gruppen kopiert werden und in eine andere Gruppe eingefügt werden. Die so eingefügte Gruppe wird als Verknüpfung der übergeordneten Gruppe angezeigt. Die Mitglieder der kopierten Gruppe erben so alle Schlüssel und Verschlüsselungsregeln der übergeordneten Gruppe. Die Voraussetzung für die Vererbung der Schlüssel ist, dass diese in der übergeordneten Gruppe als vererbbar definiert wurden. Die Rechte zum Bearbeiten der Gruppe werden hierbei NICHT vererbt.

Da die Gruppe als Verknüpfung eingefügt wurde, sind ihre Verschlüsselungsregeln, Mitglieder und Zertifikate sowie Schlüssel an dieser Stelle nicht sichtbar. Sichtbar sind diese Daten nur an der tatsächlichen Position der Gruppe in der Hierarchie. Dort können auch die so vererbten Schlüssel in Verschlüsselungsregeln verwendet werden.

Zum Hinzufügen einer Gruppe zu einer anderen über eine Referenz:

1. Markieren Sie die Gruppe und klicken Sie auf **Kopieren** im Kontextmenü.

2. Markieren Sie die Gruppe, in die Sie die Gruppe einfügen wollen und klicken Sie auf **Einfügen** im Kontextmenü. Sie können eine Referenz auch mittels „*Drag & Drop*“ bei gedrückter STRG-Taste einfügen.

3. Sie werden gefragt, ob Sie diese Gruppe einer anderen Gruppe hinzufügen wollen. Klicken Sie auf **OK**.

4. Die Gruppe wird jetzt als Verknüpfung unterhalb der Gruppe dargestellt.

Auf diese Weise können Sie ohne großen Aufwand allen Mitgliedern einer Gruppe dieselben Rechte wie den Mitgliedern einer anderen Gruppe erteilen.

Beispiel: Sollen z. B. die Mitglieder von Team „Marketing“ zur Unterstützung der Mitglieder von Team „Vertrieb“ zeitlich begrenzt auch auf deren Daten zugreifen können, ist es nur notwendig, in der Gruppe von Team „Vertrieb“ eine Verknüpfung zur Gruppe von Team „Marketing“ zu erstellen. Erzeugen Sie dann neue Profildateien. Bei der nächsten Anmeldung haben die Mitglieder von Team „Marketing“ auch Zugriff auf die Daten von Team „Vertrieb“. Sind die Arbeiten abgeschlossen, entfernen Sie einfach die Verknüpfung aus der Gruppe Team „Vertrieb“ wieder und erzeugen Sie danach neue Profildateien.

Bei der nächsten Anmeldung haben die Mitglieder von Team „Marketing“ keinen Zugriff mehr auf die Daten von Team „Vertrieb“.

3.10.5 Gruppen löschen

Einzelne Gruppen und Referenzen auf Gruppen können in der *u.trust LAN Crypt*-Administration gelöscht werden.

Zum **Löschen einer Gruppe** klicken Sie auf **Löschen** im Kontextmenü der entsprechenden Gruppe. Es werden alle Untergruppen und die Benutzermitgliedschaften gelöscht. Die Benutzer selbst werden nur gelöscht, wenn eine Gruppe in der *u.trust LAN Crypt*-Administration gelöscht wird. In diesem Fall werden auch die Mitgliedschaften der Benutzer, die eventuell in anderen Gruppen bestehen, gelöscht. Schlüssel werden NICHT gelöscht. Sie verbleiben in der *u.trust LAN Crypt*-Datenbank.

Vor dem Löschen der Gruppe wird ein Dialog angezeigt, in dem Sie das Löschen der Gruppe bestätigen müssen.

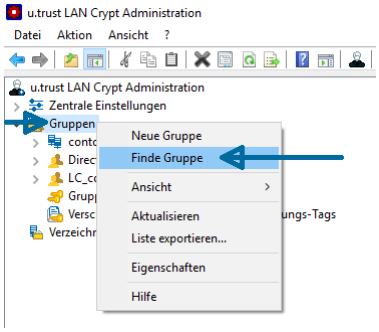
Zum **Löschen einer Referenz auf eine Gruppe** klicken Sie auf **Löschen** im Kontextmenü der entsprechenden Gruppenreferenz. Dadurch wird die Referenz gelöscht. Die Gruppe selbst wird davon nicht beeinflusst.

Vor dem Löschen der Referenz wird ein Dialog angezeigt, in dem Sie das Löschen nur dieser Referenz bestätigen müssen.

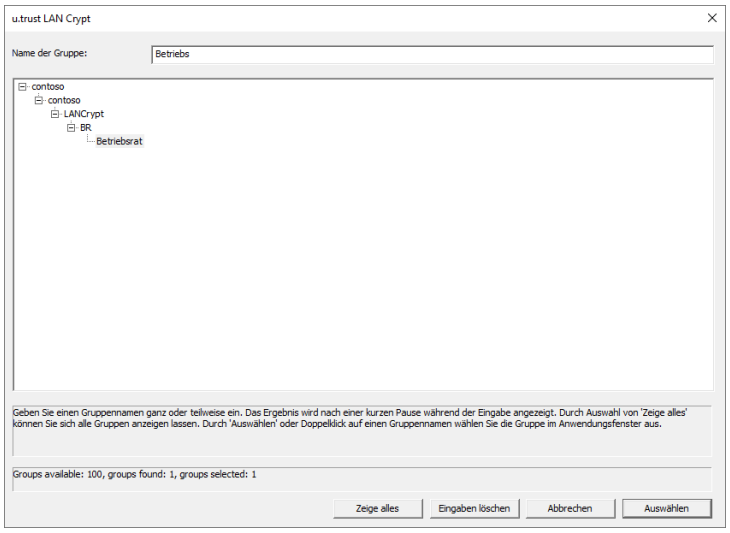
Zum Löschen aller Referenzen auf eine Gruppe steht der Befehl **Referenzen entfernen** im Kontextmenü der tatsächlichen Gruppe zur Verfügung. Klicken auf **Referenzen entfernen** löscht alle Referenzen auf die betreffende Gruppe. Die Gruppe selbst wird davon nicht beeinflusst.

3.10.6 Finde Gruppe

Sie können Gruppen mithilfe einer Suchfunktion finden. Klicken Sie hierzu mit der rechten Maustaste auf den Hauptknoten **Gruppen** und wählen Sie dort über das Kontextmenü **Finde Gruppe**.



Der folgende Dialog wird angezeigt:



Geben Sie in das Eingabefeld **Name der Gruppe** den Gruppennamen ganz oder teilweise ein, den Sie finden wollen. Das Ergebnis wird nach einer kurzen Pause während der Eingabe im Anwendungsfenster angezeigt. Durch Klicken auf **Zeige alles**, können Sie sich dort auch alle Gruppen anzeigen lassen. Markieren Sie den Gruppennamen, den Sie gesucht haben, und klicken Sie auf **Auswählen** oder Doppelklicken Sie im Anwendungsfenster auf den entsprechenden Gruppennamen, um die gewünschte Gruppe auszuwählen.

Hinweis: Die Funktion **Finde Gruppe** ist nur im Hauptknoten **Gruppen** verfügbar. In allen darunterliegenden Gruppen wird im Kontextmenü diese Funktion dagegen nicht angezeigt.

3.10.7 Gruppensymbole

Abhängig davon, von welchem Ort die OUs und Gruppen importiert worden sind, werden sie in der *u.trust LAN Crypt*-Administration mit unterschiedlichen Symbolen, wie im Folgenden dargestellt, angezeigt:

 Symbol für den Server, von dem die OUs und Gruppen importiert worden sind.

 Symbol für die Verknüpfung mit einem Server (durch Kopieren erzeugte Referenz).

 Symbol für von einem Server importierte OUs.

 Referenz auf eine importierte OU.

 Symbol für eine von einem Server importierte Gruppe.

 Referenz auf die importierte Gruppe.

 Symbol für die Datei, aus der Gruppen und Benutzer importiert wurden.

 Referenz auf die importierte Datei.

 Symbol für eine aus einer Datei importierte Gruppe.

 Referenz auf die importierte Gruppe.

 Manuell in der *u.trust LAN Crypt*-Administration angelegte Gruppe.

 Referenz auf eine manuell angelegte Gruppe.

3.11 Security Officer den Organisationseinheiten zuordnen

Nachdem OUs, Gruppen und Benutzer in die *u.trust LAN Crypt*-Administration importiert wurden, können den verschiedenen Organisationseinheiten über den Master Security Officer einzelne Security Officer zugeordnet werden.

Entsprechend der ihm erteilten Rechte, kann der Security Officer dann die Organisationseinheiten bearbeiten, denen er zugeordnet wurde.

Damit ausschließlich die Organisationseinheit, für die der Security Officer zuständig ist, für ihn bearbeitbar ist, können vom Master Security Officer die anderen Knoten für diesen Security

Officer „ausgeblendet“ werden. Das bedeutet, dass die Struktur über dem Knoten, für den der Security Officer zuständig ist, zwar als Knoten sichtbar, aber nicht bearbeitbar ist.

Wenn sich der Security Officer an die *u.trust LAN Crypt*-Administration anmeldet, dann ist ausschließlich der Teil der Organisationsstruktur sichtbar, für den der Security Officer zuständig ist.

3.11.1 Übergeordnete Gruppe eines Benutzers

Ein Benutzer kann in *u.trust LAN Crypt* Mitglied mehrerer Gruppen sein. Er hat jedoch eine bestimmte Gruppe als übergeordnete Gruppe:

- Beim Import des Benutzers über LDAP ist die übergeordnete Gruppe die OU, zu welcher der Benutzer gehört.
- Beim Import des Benutzers über eine Datei, ist die übergeordnete Gruppe die Gruppe, zu welcher der Benutzer gemäß der Definition in der Datei gehört.
- Wird ein neuer Benutzer über den Gruppeneigenschaftendialog erstellt, so ist die übergeordnete Gruppe die Gruppe, von der aus der Gruppeneigenschaftendialog geöffnet wurde.

In der u.trust LAN Crypt Admin-Konsole wird die übergeordnete Gruppe als Spalte im Knoten **Ausgewählte Benutzer und Zertifikate** oder im Knoten **Mitglieder und Zertifikate für Gruppe** angezeigt (insofern dies im Register **Benutzereinstellungen** konfiguriert ist (*siehe „Benutzereinstellungen“ auf Seite 49*).

Die übergeordnete Gruppe eines Benutzers wirkt sich in folgenden Situationen auf die Rechteauswertung aus:

- Einsehen der Eigenschaften eines Benutzers: Security Officer können die Eigenschaften eines Benutzers einsehen, wenn Sie die Rechte *Lesen* und *Sichtbar* für die übergeordnete Gruppe des Benutzers haben.
- Ändern der Eigenschaften eines Benutzers: Security Officer können die Eigenschaften eines Benutzers ändern, wenn Sie die globalen Rechte *Benutzer verwalten* und *Benutzer hinzufügen* sowie *Benutzer löschen* für die übergeordnete Gruppe des Benutzers haben.
- Erzeugen von Profilen: Wenn das Recht *Profile erzeugen* für eine Gruppe für einen Security Officer gesetzt ist, darf der Security Officer Profile für alle Mitglieder der Gruppe erstellen, für die die Gruppe auch das übergeordnete Objekt der Gruppe ist. Der Security Officer darf keine Profile für Benutzer erstellen, die nur Mitglieder der Gruppe sind und eine andere übergeordnete Gruppe haben. Hierfür ist die Berechtigung *Profile für alle Mitglieder erzeugen* erforderlich.
- Zuweisen von Zertifikaten: Wenn das Recht *Zertifikate zuweisen* für eine Gruppe gesetzt ist, darf der Security Officer allen Mitgliedern der Gruppe Zertifikate zuweisen, für die die Gruppe auch das übergeordnete Objekt der Gruppe ist. Der Security Officer darf keine Zertifikate zu Benutzern zuweisen, die nur Mitglieder der Gruppe sind und eine andere

übergeordnete Gruppe haben. Hierfür ist das Recht *Zertifikate allen Mitgliedern zuweisen* erforderlich.

- Kopieren von Benutzern: Wenn ein Security Officer einen Benutzer zu einer Gruppe über den Eigenschaftendialog einer Gruppe hinzufügen will (im Register **Mitglieder** über die Schaltfläche **Hinzufügen**), muss der Security Officer das Recht *Benutzer kopieren* für die übergeordnete Gruppe des Benutzers besitzen.

3.11.2 Gruppen für einen Security Officer sichtbar und bearbeitbar machen

1. Damit ein Knoten in der Administration für einen Security Officer sichtbar wird, muss zuerst beim Basisknoten der Organisationsstruktur das Recht **Sichtbar** gesetzt werden.

2. Markieren Sie dazu den Basisknoten der Struktur und öffnen Sie durch Klicken auf **Eigenschaften** im Kontextmenü den *Eigenschaften*-Dialog für diesen Knoten.

3. Wechseln Sie zum Register **Sicherheit** und klicken Sie auf **Hinzufügen**.

   Sie können hier den Security Officer auswählen, den Sie zur Bearbeitung der Gruppen vorgesehen haben.

   Hinweis: Einer Gruppe können mehrere Security Officer zugeteilt werden.

4. Durch Klicken auf **Weiter** wird der *Rechte*-Dialog für diesen Security Officer geöffnet. Wählen Sie an dieser Stelle nur das Recht *Sichtbar* aus und klicken Sie auf **Fertigstellen**. Dieses Recht wird in der Gruppenhierarchie nach unten vererbt und Sie haben damit für den Security Officer alle Gruppen sichtbar gemacht.

   Sollte sich der Security Officer mit diesen Einstellungen an die Datenbank anmelden, würde er die gesamte Struktur in der Administration zwar sehen, diese aber nicht bearbeiten können.

5. Im nächsten Schritt können Sie nun die Gruppen, an denen der Security Officer keine Rechte haben soll und diese auch in seiner Administration nicht sehen soll, ausblenden.

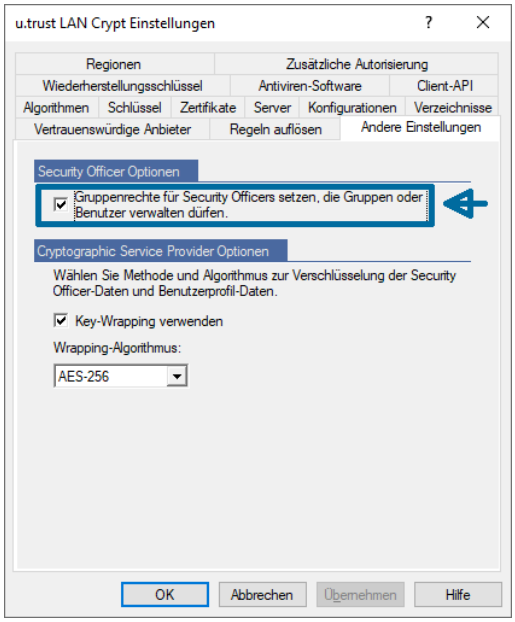
6. Markieren Sie hierzu die entsprechenden Gruppen, öffnen Sie deren *Eigenschaften*-Dialoge und wechseln Sie zum Register **Sicherheit**.

7. Setzen Sie bei den Gruppen, die für den Security Officer nicht sichtbar sein sollen, das Recht *Sichtbar* auf *Verweigern*.

Hinweis: Wurde einem Security Officer explizit ein Recht auf einer übergeordneten Gruppe verweigert, ist eine Zulassung dieses Rechts in einer untergeordneten Gruppe ebenfalls nicht möglich. Es wird daher empfohlen, einem Security Officer auf einer übergeordneten Gruppe lediglich die Rechte *Lesen* und *Sichtbar* zu erteilen, damit in untergeordneten Gruppen die Rechtevergabe problemlos möglich ist.

Hinweis: *u.trust LAN Crypt* kann so konfiguriert werden, dass automatisch eine ACL mit Leserechten für die Stammgruppe für einen neu erstellten Security Officer angelegt wird. Hierbei ist erforderlich, dass der Security Officer das globale Recht *Gruppen verwalten* oder *Benutzer verwalten* hat. Dadurch wird garantiert, dass der Security Officer Zugriff (einsehen und / oder bearbeiten) auf die Gruppen hat, für die er verantwortlich ist. Dieses Verhalten muss im Register **Andere Einstellungen** unter dem Knoten **Zentrale Einstellungen** aktiviert werden.

Beispiel (Master Security Officer):



Für den Security Officer ergäbe sich mit diesen Einstellungen bei der Anmeldung folgendes Szenario:

Es werden nur die Gruppen angezeigt, für die der Security Officer das Recht *Sichtbar* besitzt. Diese Gruppen werden grau dargestellt, da dem Security Officer noch keine Rechte zur Bearbeitung der Gruppen zugeteilt wurden.

Wird dem Security Officer gleichzeitig mit dem Recht *Sichtbar* auch das Recht *Lesen* erteilt, würden unter den Gruppen auch die Snap-Ins für *Verschlüsselungsregeln*, *Mitglieder und Zertifikate für Gruppe* und *Gruppenschlüssel* angezeigt werden. Der Security Officer könnte zwar die Inhalte der Snap-Ins sehen, wäre aber noch nicht in der Lage, diese zu bearbeiten.

Das Recht *Lesen* ermöglicht es, einem Security Officer Informationen über andere Gruppen zu geben, ohne dass er diese bearbeiten darf, indem sie in seiner Ansicht einfach eingeblendet werden.

Hinweis: Wurde dem Security Officer auch das Recht *Lesen* erteilt, so muss es explizit verweigert werden, um die Gruppen wieder auszublenden. Es genügt nicht, nur das Recht *Sichtbar* zu verweigern.

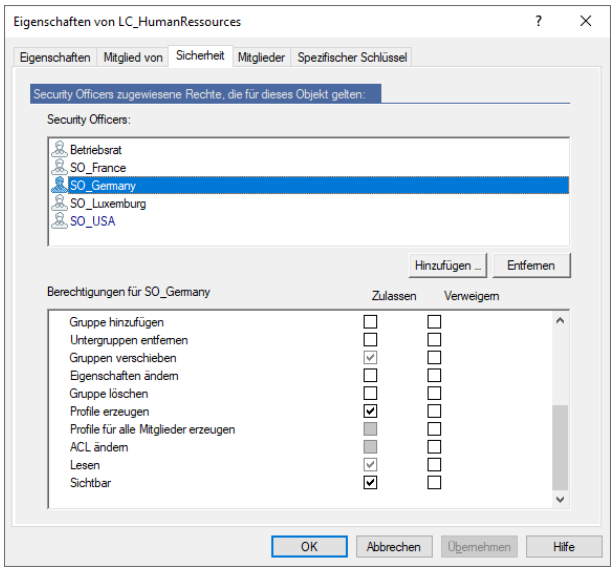
3.11.3 Dem Security Officer Rechte zur Bearbeitung der Gruppen zuweisen

Nachdem für den Security Officer die Gruppen sichtbar sind, die er bearbeiten soll, können ihm die entsprechenden Rechte zugeteilt werden.

Diese Rechte werden von oben nach unten in der Hierarchie vererbt und können an einer weiter unten gelegenen Stelle wieder verweigert werden.

1. Markieren Sie die Gruppe, für die Sie dem Security Officer Rechte zuteilen wollen, öffnen Sie den Dialog *Eigenschaften* und wechseln Sie zum Register **Sicherheit**.

2. Unter *Security Officers* werden alle Security Officer angezeigt, die dieser Gruppe zugeteilt sind. Wenn Sie dort einen Security Officer auswählen, werden dessen geltende Berechtigungen im unteren Teil des Dialogs angezeigt.



Aus einer anderen Gruppe **vererbte Rechte** sind durch ein graues Häkchen gekennzeichnet. Bei Rechten, die aufgrund der Einstellungen in den globalen Rechten nicht vergeben werden können, ist das Kontrollkästchen ganz ausgegraut.

Hinweis: Die für den Security Officer zur Verfügung stehenden Rechte sind abhängig von den Einstellungen bei den globalen Rechten. Die globalen Rechte wurden bereits bei der Erzeugung des Security Officers festgelegt.

Hinweis: Klicken Sie auf **Zulassen / Verweigern**, um alle Rechte in einem Schritt zuzulassen bzw. zu verweigern. Ein weiterer Klick hebt die Auswahl aller Rechte wieder auf. Sind alle Rechte markiert, können sie anschließend selektiv wieder ein- bzw. ausgeschaltet werden. Ausgegraute Rechte können dem Security Officer aufgrund anderer Einstellungen nicht zugestanden werden.

Hinweis: Siehe auch „*Gruppenrechte für Security Officers setzen, die Gruppen oder Benutzer verwalten dürfen*“ auf Seite 83.

Folgende Rechte können vergeben werden:

Rechte	Beschreibung
Schlüssel erzeugen	Der Security Officer darf Schlüssel in der Gruppe erzeugen.
Schlüssel kopieren	Der Security Officer darf Schlüssel kopieren.
Schlüssel entfernen	Der Security Officer darf Schlüssel entfernen.
Regeln erzeugen	Der Security Officer darf Verschlüsselungsregeln erzeugen.
Zertifikate zuweisen	Der Security Officer darf den Benutzern Zertifikate zuweisen. Der Security Officer darf den Assistenten zur Zertifikatszuweisung starten. Diese Berechtigung erlaubt es dem Security Officer, den Benutzern in der Gruppe Zertifikate zuzuweisen, wenn die Gruppe auch die übergeordnete Gruppe ist.
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung *Zertifikate zuweisen* gesetzt ist. *Zertifikate allen Mitgliedern zuweisen* berechtigt einen Security Officer zum Zuweisen von Zertifikaten zu Benutzern, wenn der Security Officer die Berechtigung *Zertifikate zuweisen* für die übergeordnete Gruppe des Benutzers oder die Berechtigung *Zertifikate allen Mitgliedern zuweisen* für eine Gruppe, welcher der Benutzer angehört, hat. **Beachten Sie:** Wenn Sie *Zertifikate allen Mitgliedern zuweisen* auf **Zulassen** setzen, wird die Berechtigung *Zertifikate zuweisen* automatisch auf **Zulassen** gesetzt. Wenn Sie die Berechtigung *Zertifikate zuweisen* auf **Verweigern** setzen, wird auch die Berechtigung *Zertifikate allen Mitgliedern zuweisen* auf **Verweigern** gesetzt.

Rechte	Beschreibung
Benutzer hinzufügen	Der Security Officer darf manuell Benutzer zur Gruppe hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Benutzer kopieren	Der Security Officer darf Benutzer zu Gruppen hinzufügen (kopieren). Dies ist nur denjenigen Mitgliedern erlaubt, für die diese Gruppe auch das übergeordnete Objekt ist.
Benutzer löschen	Der Security Officer darf Benutzer über das Snap-In *Mitglieder und Zertifikate für Gruppe* löschen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Gruppe hinzufügen	Der Security Officer darf über das Kontextmenü einer Gruppe neue Gruppen hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Untergruppe entfernen	Der Security Officer darf Untergruppen dieser Gruppe entfernen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Gruppen verschieben	Der Security Officer darf manuell angelegte Gruppen in der Administration (mit *Drag & Drop*) verschieben. Importierte Gruppen können nicht verschoben werden. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Eigenschaften ändern	Der Security Officer darf die Eigenschaften der Gruppe ändern
Gruppe löschen	Der Security Officer darf Gruppen löschen. Dies setzt voraus, dass er in der übergeordneten Gruppe das Recht Untergruppe entfernen hat. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.

Rechte	Beschreibung
Profile erzeugen	Der Security Officer darf den Profile Resolver starten und Profildateien für ausgewählte Benutzer erstellen. Profile erzeugen berechtigt den Security Officer, Profile für Benutzer zu erstellen, für die die Gruppe auch die übergeordnete Gruppe ist.
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Profile erzeugen gesetzt ist. Profile für alle Mitglieder erzeugen berechtigt den Security Officer dazu, Profile für alle Benutzer in der Gruppe zu erzeugen: Benutzer, für die die Gruppe auch die übergeordnete Gruppe ist, und für Benutzer, die Mitglieder der Gruppe sind, die jedoch eine andere übergeordnete Gruppe haben. **Beachten Sie:** Wenn Sie *Profile für alle Mitglieder erzeugen* auf **Zulassen** setzen, wird die Berechtigung *Profile erzeugen* automatisch auf **Zulassen** gesetzt. Wenn Sie *Profile erzeugen* auf **Verweigern** setzen, wird die Berechtigung *Profile für alle Mitglieder erzeugen* automatisch auf **Verweigern** gesetzt.
ACL ändern	Der Security Officer darf die ACL dieser Gruppe ändern (z. B. einen anderen Security Officer hinzufügen).
Lesen	Der Security Officer hat Leserechte an dieser Gruppe; er kann den Inhalt der Snap-Ins sehen. Diese Einstellung wird automatisch gesetzt, wenn Bearbeitungsrechte vergeben werden.
Sichtbar	Die Gruppe ist für den Security Officer sichtbar. Dies wird am Basisknoten gesetzt und nach unten vererbt. Wird es dem Security Officer verweigert, wird die Gruppe ausgeblendet (auch *Lesen* muss hierbei verweigert sein).

3. Wählen Sie die Rechte aus, die Sie dem Security Officer zuteilen wollen. **Übernehmen** speichert die Einstellungen in der Datenbank.

4. Haben Sie dieser Gruppe weitere Security Officer zugeordnet, können Sie jetzt auch deren Rechte einstellen. Markieren des SOs unter *Security Officers* zeigt dessen eingestellte Rechte an.

Hinweis: Änderungen an den Berechtigungen eines Security Officers für eine Gruppe werden erst wirksam, wenn der Security Officer sich erneut an der *u.trust LAN Crypt* Admin-Konsole angemeldet hat.

3.12 Eigenschaften von Gruppen

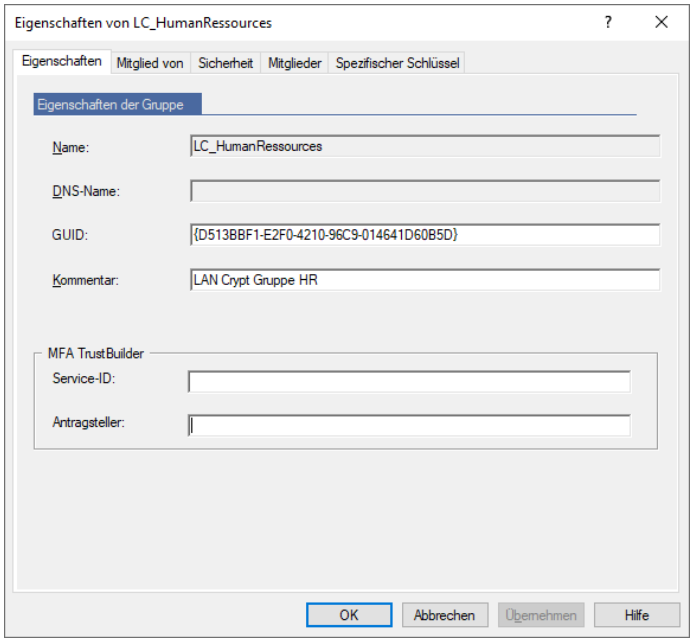
Der Dialog *Eigenschaften* einer Gruppe (<Gruppe> / Kontextmenü / Eigenschaften) besteht aus vier Registern, auf deren Seiten die Eigenschaften der Gruppe bearbeitet werden können.

3.12.1 Der Reiter Eigenschaften

Der Reiter Eigenschaften zeigt

- Name
- DNS-Name
- GUID
- Kommentar
- Service-ID (MFA TrustBuilder)
- Antragsteller (MFA TrustBuilder)

zur Gruppe an.



Multi-Faktor-Authentifizierung (MFA) mit TrustBuilder

Durch die Unterstützung von MFA (**M**ulti-**F**aktor-**A**uthentifizierung) können sich Benutzer auf besonders sichere Weise am *u.trust LAN Crypt* Client anmelden. Die Anmeldung selbst erfolgt dann mithilfe eines zweiten Gerätes (das kann z. B. das Smartphone oder Tablet des Benutzers sein). Die Einstellungen von *TrustBuilder* werden durch den Windows- oder *TrustBuilder*-Administrator konfiguriert. Setzen Sie sich mit diesem in Verbindung und fragen Sie nach den benötigten Angaben *Service-ID* und *Antragsteller* für die *MFA TrustBuilder*-Einstellungen für *u.trust LAN Crypt*.

Tragen Sie in das Feld *Service-ID* die erforderliche Nummer und in das Feld *Antragsteller* das API-Zertifikat („*@cert.trustbuilder*“) des *TrustBuilder-Services* ein.

Hinweis: Damit die Benutzer der Gruppe *TrustBuilder MFA* nutzen können, muss für sie das Profil neu erzeugt werden (siehe „*Bereitstellen der Verschlüsselungsregeln - Profildateien erzeugen*“ auf Seite 166). Nach dem Laden des neuen Profils können die Benutzer ihre Anmeldung am *u.trust LAN Crypt* Client über *TrustBuilder MFA* durchführen. Der Benutzer erhält dann eine Authentifizierungsaufforderung auf seinem registrierten MFA-Token (z. B. sein Smartphone), gibt dort seine PIN ein, bestätigt diese und wird dann am *u.trust LAN Crypt* Client angemeldet.

Hinweis: Beachten Sie hierbei, dass das API-Zertifikat des *TrustBuilder*-Dienstes im Zertifikatsspeicher des Benutzers beim *u.trust LAN Crypt* Client installiert sein muss.

Hinweis: Definieren Sie für eine Gruppe Angaben für eine Multi-Faktor-Authentifizierung (MFA), werden diese nicht nach unten vererbt. Sie müssen diese also explizit für jede Gruppe einzeln definieren.

3.12.2 Der Reiter Mitglied von

Auf dem Reiter **Mitglied von** werden jene Gruppen angezeigt, in denen die aktuelle Gruppe Mitglied ist.

3.12.3 Mitglieder hinzufügen / entfernen

Auf dem Reiter **Mitglieder** können der aktuellen Gruppe Mitglieder hinzugefügt werden. In der Liste werden alle vorhandenen Benutzer und Gruppen, die Mitglieder dieser Gruppe sind, angezeigt. Es können nur die aufgelisteten Benutzer bearbeitet werden, keine Gruppen!

Hinzufügen:

Öffnet einen Dialog, in dem Benutzer ausgewählt werden können, die dann der Gruppe hinzugefügt werden können.

Es werden entweder alle Benutzer angezeigt oder es können Benutzergruppen bzw. einzelne Benutzer mithilfe von SQL-Platzhaltern ausgewählt werden.

Da das Anzeigen aller Benutzer sehr zeitaufwendig werden kann, ermöglicht *u.trust LAN Crypt* das Einschränken der Suche durch die Definition von Suchkriterien.

Durch Auswählen der Option *Passende Benutzer anzeigen* werden die Eingabefelder zum Festlegen der Suchkriterien aktiviert.

Die folgenden Informationen über die Benutzer werden aus der *u.trust LAN Crypt*-Datenbank ermittelt:

- Anmeldename
- Benutzername
- Zuordnung zwischen Benutzer und Zertifikat
- Antragssteller des Zertifikats
- Seriennummer des Zertifikats
- Datum, ab welchem das Zertifikat gültig ist
- Datum, bis zu dem das Zertifikat gültig ist
- Name der Elterngruppe

Basierend auf diesen Attributen können die Suchkriterien angegeben werden. *u.trust LAN Crypt* sucht nach festgelegten Zeichenketten in den ausgelesenen Attributen der Benutzer.

In der ersten Dropdownliste können Sie auswählen, auf welche/welches Attribut/e die Suche angewendet werden soll.

Daneben können Sie festlegen, ob die Zeichenkette enthalten sein soll (*soll sein*) oder ob nur Benutzer angezeigt werden, in denen die Zeichenkette im ausgewählten Attribut nicht enthalten sein darf (*darf nicht sein*).

In das Feld ganz rechts können Sie die eigentliche Zeichenkette eingeben, nach der *u.trust LAN Crypt* beim ausgewählten Attribut suchen soll.

Zur Angabe der Zeichenkette können Sie folgende SQL-Platzhalter verwenden:

%	beliebige Zeichenfolge
_	einzelnes Zeichen (beispielsweise bedeutet „*a__*“: Suche nach allen Namen mit drei Buchstaben, die mit „a“ beginnen)
[]	einzelnes Zeichen aus einer Liste (z. B. „*[a-cg]%*“ bedeutet: Suche nach allen Namen, die mit „a, b, c oder g“ beginnen)
[^]	einzelnes Zeichen, das nicht in einer Liste ist (z. B. „*[^a]%*“ bedeutet: Suche nach allen Namen, die mit „a“ beginnen)

Sie können bis zu drei Bedingungen für die Suche angeben. Geben Sie mehr als eine Bedingung an, können Sie festlegen, wie diese Bedingungen verknüpft werden sollen (UND / ODER).

Durch Klicken auf **OK** werden alle in der Liste markierten Benutzer der aktuellen Gruppe hinzugefügt.

Neu:

Öffnet einen Dialog, in dem ein neuer Benutzer angelegt werden kann.

Löschen:

Löscht die ausgewählte Benutzermitgliedschaft aus der aktuellen Gruppe.

Wenn der Benutzer keiner weiteren Gruppe angehört, wird er aus der *u.trust LAN Crypt*-Datenbank gelöscht.

Insofern der Benutzer mehreren Gruppen angehört, und es sich bei der aktuellen Gruppe um die übergeordnete Gruppe des Benutzers handelt, hängt die resultierende Aktion vom Typ der Gruppe ab:

- Wenn es sich bei der Gruppe um eine Organisationseinheit (OU) oder eine Stammgruppe handelt und der Benutzer Mitglied einer anderen OU oder Stammgruppe ist, wird diese OU oder Stammgruppe zur übergeordneten Gruppe des Benutzers. Wenn keine andere OU oder Stammgruppe vorhanden ist, der der Benutzer angehört, wird der Benutzer gelöscht (im Vergleich ist das ähnlich wie beim Active Directory oder bei Novell. Auch hier wird der Benutzer gelöscht, wenn die OU, der er angehört, gelöscht wird).

- Wenn es sich bei der Gruppe um eine einfache Gruppe (keine OU oder Stammgruppe) handelt, wird eine der anderen Gruppen, denen der Benutzer angehört, zur übergeordneten Gruppe des Benutzers.

Eigenschaften:

Zeigt die Eigenschaften des markierten Benutzers an.

Hinweis: Ein Benutzer darf in einem Container genau einmal vorhanden sein. Wird versucht, einen Benutzer in einem Container anzulegen / hinzuzufügen, obwohl dieser darin bereits enthalten ist, wird eine Meldung angezeigt, dass dies nicht möglich ist.

Es kann im System jedoch mehrere Benutzer geben, die den gleichen Namen haben, solange sie sich nicht im selben Container befinden.

3.12.4 Security Officer hinzufügen

Über den Reiter **Sicherheit** kann auch ein (Master) Security Officer der aktuellen Gruppe weitere Security Officer hinzufügen und ihnen Rechte an der Gruppe zuweisen (siehe Abschnitt 3.11.3 „*Dem Security Officer Rechte zur Bearbeitung der Gruppen zuweisen*“ auf Seite 121). Voraussetzung dafür ist, dass dann der Security Officer, der einen weiteren Security Officer hinzufügen will, das globale Recht **ACL ändern** besitzt. Ein Master Security Officer dagegen besitzt dieses Recht immer.

Hinweis: Ein Security Officer kann einen anderen Security Officer, den er der Gruppe hinzufügt, nur mit Rechten ausstatten, über die er auch selbst verfügt.

Ein Security Officer kann sich selbst nicht in ACLs aufnehmen oder seine eigenen Rechte in einer ACL bearbeiten.

3.13 Eigenschaften von Benutzern

Der Dialog *Eigenschaften* eines Benutzers (<Benutzer> / Kontextmenü / Eigenschaften) besteht aus vier Reitern, auf deren Seiten die Eigenschaften des Benutzers bearbeitet werden können.

Zertifikate

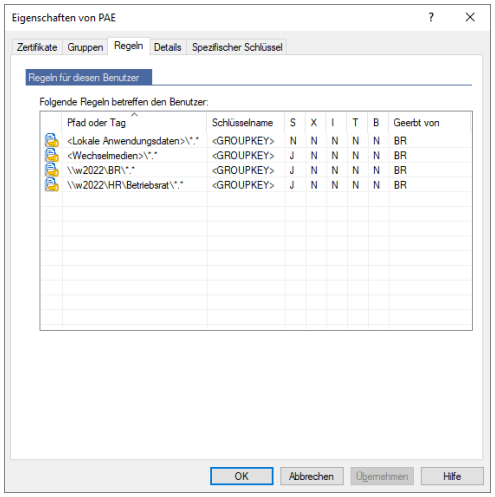
Im Reiter **Zertifikate** werden alle Zertifikate, die dem Benutzer zugeordnet sind, angezeigt. An dieser Stelle kann auch ein neues *LAN Crypt*-Zertifikat für den Benutzer erzeugt, ein bereits vorhandenes Zertifikat aus dem Zertifikatsspeicher hinzugefügt oder auch ein Zertifikat aus einer Datei importiert werden (siehe *Zertifikat einem Benutzer zuordnen* auf Seite 158).

Gruppen

Im Reiter **Gruppen** werden jene Gruppen angezeigt, in denen der Benutzer Mitglied ist. Zudem können Sie Mitgliedschaften des Benutzers zu Gruppen entfernen oder auch neue hinzufügen.

Regeln

Im Reiter **Regeln** werden alle Verschlüsselungsregeln des Benutzers angezeigt. Sie erhalten dort einen schnellen Überblick über alle Regeln, die für diesen Benutzers gelten, auch wenn diese aus verschiedenen Gruppen stammen.



Die Spalten S, X, I, T, B geben Auskunft, um welche Art von Regel es sich handelt:

- **S** (Subdirectories): Unterverzeichnisse bzw. Unterordner werden ebenfalls verschlüsselt.
- **X** (Exclude path): Der Pfad wird von der Verschlüsselung ausgenommen.
- **I** (Ignore path): Der Pfad wird von *u.trust LAN Crypt* ignoriert. Weitere Informationen, siehe „*Erzeugen von Verschlüsselungsregeln*“ auf Seite 145.
- **T** (Tag): Das Tag wird von der *u.trust LAN Crypt* Client-API als vordefiniertes Verschlüsselungs-Tag verwendet (siehe *Verschlüsselungs-Tags* auf Seite 156).
- **B** (Bypass): Der Pfad ist als *Bypass-Regel* definiert (siehe „*Bypass-Regel setzen*“ auf Seite 152).

Unterhalb der Spalte **Geerbt von** ist ersichtlich, aus welchen Gruppen die einzelnen Regeln geerbt wurden.

Alternativ können Sie sich diese Informationen auch beim *u.trust LAN Crypt*-Client in der Profilansicht eines Benutzers anzeigen lassen.

Details

Im Reiter **Details** werden die Daten des Benutzers angezeigt und können dort bearbeitet werden.

Sie können in das Eingabefeld *E-Mail-Adresse* die E-Mail-Adresse des Benutzers eintragen. Diese wird dann auch in die Passwortprotokolldatei für von *u.trust LAN Crypt* erzeugte Zertifikate eingetragen. Auf diese Weise kann sie beispielsweise für die Erstellung eines PIN-Mailers via E-Mail verwendet werden.

Hinweis: E-Mail-Adressen der Benutzer dürfen keine Zeichen oberhalb des ASCII-Codes 127 enthalten und somit auch keine Umlaute. Am Anfang und Ende der Zeichenkette darf sich kein Punkt befinden.

Im Abschnitt *MFA TrustBuilder* können Sie die Angaben für die **M**ulti-**F**aktor-**A**uthentifizierung für einzelne Benutzer mit TrustBuilder definieren.

Setzen Sie sich hierzu mit Ihrem Windows-Administrator in Verbindung, der für die Administration von *TrustBuilder* zuständig ist und fragen Sie diesen nach den erforderlichen Angaben. Tragen Sie die erforderliche Nummer für die *Service-ID*, die *Benutzer-ID* und den *Antragsteller* ("*@cert.trustbuilder*", das API-Zertifikat des TrustBuilder-Services) in die jeweiligen Felder ein.

Weitere Informationen hierzu und wie Sie diese Einstellung für alle Benutzer einer Gruppe definieren, finden Sie im Reiter *Eigenschaften* der jeweiligen Gruppen (siehe „*TrustBuilder MFA und u.trust LAN Crypt*“ auf Seite 125).

Hinweis: Bitte gehen Sie bei einer eventuellen Änderung der Benutzerdaten vorsichtig vor. Es können dabei leicht unerwünschte Nebeneffekte auftreten. Zum Beispiel kann eine Änderung des Anmeldenamens an dieser Stelle bewirken, dass der Benutzer danach keinen Zugriff auf seine Profildatei mehr hat, da der Client nach einer Profildatei mit einem anderem - dem zuvor verwendeten - Anmeldenamen sucht.

Hinweis: Wenn Sie über einen Registry-Eintrag das Zuweisen „spezifischer Schlüssel“ konfiguriert haben, wird ein weiterer Reiter „**Spezifischer Schlüssel**“ angezeigt (siehe „Spezifische Schlüssel wieder zuweisen“ auf Seite 135).

3.14 Design der Sicherheitsumgebung

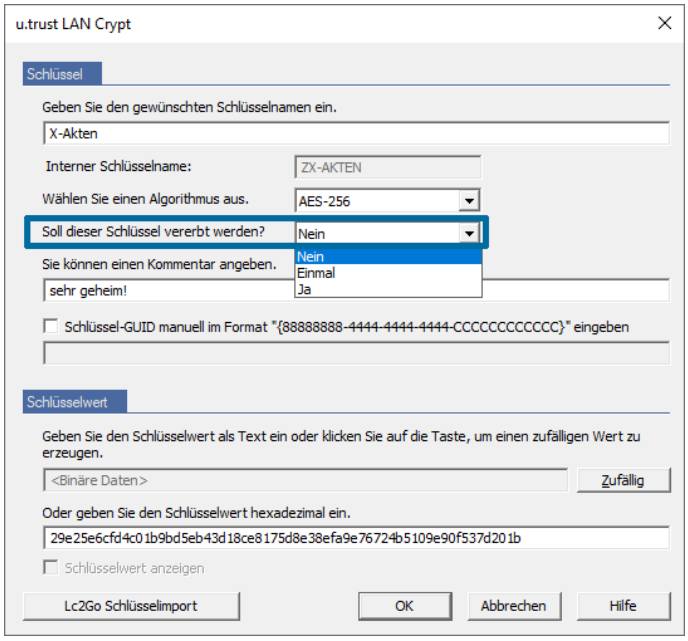
Durch seine große Flexibilität ist es möglich, *u.trust LAN Crypt* an die Sicherheitserfordernisse jedes Unternehmens anzupassen.

Doch ist es von großer Bedeutung, eine unternehmensweite Sicherheitsstrategie zu entwerfen, bevor die *u.trust LAN Crypt*-Umgebung aufgebaut wird.

Generell ist zu empfehlen, mit einer eher restriktiven Sicherheitsrichtlinie zu beginnen, da es leichter ist, diese zu lockern, als hinterher eine strengere Sicherheitsrichtlinie im *u.trust LAN Crypt*-System einzuführen. Im letzteren Fall können Sicherheitsprobleme auftreten, die nicht leicht zu lösen sind. Um dies zu vermeiden, ist es äußerst wichtig, eine unternehmensweit geltende Sicherheitsrichtlinie zu definieren, bevor mit dem Erzeugen und Verteilen der Verschlüsselungsprofile über die Profildateien begonnen wird.

3.15 Schlüssel erzeugen

Neue Schlüssel werden unter dem Gruppenknoten der Gruppe erzeugt, für die sie verwendet werden sollen. Für jeden Schlüssel kann festgelegt werden, ob er in der Hierarchie der Gruppen nach unten vererbt werden soll.



Hinweis: Alle in der *u.trust LAN Crypt*-Datenbank vorhandenen Schlüssel werden im Knoten **Zentrale Einstellungen** und dort unter dem Knoten **Alle u.trust LAN Crypt Schlüssel** angezeigt. Sie können an dieser Stelle aber nicht bearbeitet werden. Diese Ansicht stellt nur einen Überblick über die in *u.trust LAN Crypt* verwendeten Schlüssel dar. **Schlüssel können grundsätzlich nur in den Gruppen bearbeitet werden, in denen sie auch erzeugt wurden.**

Hinweis: Ein Security Officer, der das Recht **Profile erzeugen** nicht hat, sondern nur das Recht **Schlüssel erzeugen**, darf beim Anlegen des Schlüssels keinen Wert vergeben! Der Wert wird bei der ersten Übertragung des Schlüssels in ein Profil automatisch erzeugt.

Ein *u.trust LAN Crypt*-Schlüssel besteht aus den folgenden Komponenten:

- **Name**

  Im Sinne einer besseren Übersichtlichkeit ist es empfehlenswert, dass der Name der Benutzergruppe Teil des Schlüsselnamens ist.

  Da *u.trust LAN Crypt* auch die Möglichkeit bietet, Schlüssel zu sortieren, kommt der Namensgebung eine besondere Bedeutung zu.

  u.trust LAN Crypt erzeugt aus dem angegebenen Schlüsselnamen einen 16 Zeichen langen Schlüsselnamen zur internen Verwendung. Wird der Schlüssel für eine Region erstellt, erhält der Schlüsselname das für diese Region definierte Präfix vorangestellt.

- **Schlüsselwert**

  Die Länge des Schlüssels ist abhängig vom gewählten Algorithmus. Der Schlüsselwert kann entweder in ANSI-Zeichen oder in Hexadezimal-Notation (erlaubte Zahlen bzw. Zeichen: 0123456789abcdef) eingegeben werden. Der jeweils andere Wert wird automatisch ergänzt.

  Es muss kein Schlüsselwert angegeben werden. In diesem Fall wird der Wert zufällig erzeugt, sobald der Schlüssel das erste Mal in einem Benutzerprofil verwendet wird.

- **Verschlüsselungsalgorithmus**

  AES-128, AES-256, DES, 3DES, IDEA, XOR

- **Kommentar** (optional)

- **Schlüssel-GUID** (optional)

  Ermöglicht die manuelle Eingabe einer Schlüssel-GUID, um verschlüsselte Dateien zwischen zwei oder mehr unterschiedlichen *u.trust LAN Crypt*-Installationen austauschen zu können (siehe „*Schlüssel*“ auf Seite 52).

  Bleibt das Feld leer, wird automatisch eine GUID gebildet.

Um einen neuen Schlüssel zu erzeugen:

1. Markieren Sie **Gruppenschlüssel** unter der Gruppe, für die Sie einen Schlüssel erzeugen wollen.

2. Klicken Sie auf das gelbe Schlüsselsymbol in der Symbolleiste oder klicken Sie nach einem Rechtsklick im rechten Fenster der Konsole auf **Neuer Schlüssel** im Kontextmenü.

3. Geben Sie einen Namen für den neuen Schlüssel in das oberste Eingabefeld ein. Backslash (\), Slash (/), Hochkomma und das „&“-Zeichen sind keine gültigen Zeichen für Schlüsselnamen. *u.trust LAN Crypt* erzeugt aus diesem Namen einen 16 Zeichen langen eindeutigen Schlüsselnamen zur internen Verwendung. Dabei wird diesem eindeutigen Namen das Präfix für die Region (falls dieses in den Eigenschaften des Security Officers angegeben wurde) vorangestellt. Der interne Name wird rechts, neben der Dropdownliste, zur Auswahl des Algorithmus angezeigt.

Der Schlüsselname kann später geändert werden (im **Eigenschaften** Dialog des betreffenden Schlüssels), der daraus erzeugte interne Name nicht.

4. Wählen Sie einen Verschlüsselungsalgorithmus aus der Dropdownliste aus.

   Es werden hier nur die Algorithmen, die Sie im Register **Algorithmen** im Eigenschaften-Dialog des Knotens **Zentrale Einstellungen** als verfügbar angegeben haben, angezeigt.

   Hinweis: Bitte wählen Sie zum Verschlüsseln Ihrer Daten immer einen sicheren Algorithmus, wie z. B. AES-256 oder AES-128, da ältere Verschlüsselungsalgorithmen, wie z. B. XOR, IDEA, DES oder 3DES, als nicht mehr sicher gelten.

5. Geben Sie an, ob der Schlüssel an die Untergruppen vererbt werden soll:

   - **Nein**

     Der Schlüssel wird nicht vererbt und steht damit nur in der aktuellen Gruppe zur Verfügung.

   - **Einmal**

     Der Schlüssel wird in die Gruppe(n), die sich eine Hierarchieebene unter der aktuellen Gruppe befinden, vererbt.

   - **Ja**

     Der Schlüssel wird an alle Gruppen, die sich unterhalb dieser Gruppe befinden, vererbt und steht dort zum Erzeugen der Verschlüsselungsregeln zur Verfügung.

6. Im nächsten Eingabefeld können Sie einen Kommentar zu diesem Schlüssel eingeben.

7. Aktivieren Sie bei Bedarf das Kontrollkästchen **Schlüssel-GUID manuell im Format 88888888-4444-4444-4444-CCCCCCCCCCCC eingeben** und geben Sie die gewünschte GUID ein (setzt aktivierte Option "Security Officers dürfen die GUID neuer Schlüssel festlegen" in den Einstellungen im Knoten **Zentrale Einstellungen** voraus). Die voreingestellte GUID `88888888-4444-4444-4444-CCCCCCCCCCCC` kann hier nicht einfach übernommen werden. Sie muss in jedem Fall angepasst werden.

8. Im Abschnitt *Schlüsselwert* geben Sie den Schlüsselwert als Text ein oder klicken Sie auf die Taste, um einen zufälligen Wert zu erzeugen. Der jeweils andere Wert wird automatisch ergänzt. Oder klicken Sie auf die Schaltfläche **Zufällig** (empfohlen), um *u.trust LAN Crypt* einen zufälligen Wert berechnen zu lassen.

9. Alternativ geben Sie den Schlüsselwert hexadezimal (Buchstaben A-F, Ziffern 0-9) in das Eingabefeld darunter ein und klicken Sie dann auf **OK**.

Der neue Schlüssel wird in der Schlüsselansicht der Konsole angezeigt.

3.15.1 Lc2Go Schlüsselimport

Sie können Schlüssel aus Dateien importieren, die mit Lc2Go verschlüsselt sind. Klicken Sie hierzu auf die Schaltfläche **Lc2Go Schlüsselimport**. Wählen Sie danach eine mit Lc2Go verschlüsselte Datei aus, deren Schlüssel Sie nach *u.trust LAN Crypt* importieren wollen.

Klicken Sie ggf. auf **Durchsuchen** ("..."), wenn Sie die mit Lc2Go verschlüsselte Datei von einem bestimmten Pfad mithilfe des Dateiexplorers auswählen und importieren möchten.

Geben Sie die dazugehörige Passphrase (das sichere Kennwort) für die Datei in das Eingabefeld **Passphrase** ein.

Der importierte Lc2Go-Schlüssel wird in der Schlüsselansicht der Konsole angezeigt und kann danach für Verschlüsselungsregeln verwendet werden.

3.15.2 Spezifische Schlüssel

Neben den so erzeugten Schlüsseln bietet *u.trust LAN Crypt* auch die Möglichkeit, benutzer- bzw. gruppenspezifische Schlüssel zu verwenden.

<USERKEY>

Beim Erzeugen der Verschlüsselungsregeln wird in der Liste der Schlüssel auch immer ein Schlüssel **<USERKEY>** angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.

<GROUPKEY>

Analog zur Verwendung von **<USERKEY>** kann durch die Verwendung von **<GROUPKEY>** ein gruppenspezifischer Schlüssel für alle Mitglieder einer Gruppe erzeugt werden. Bei der Auflösung der Verschlüsselungsregeln wird der Gruppenschlüssel automatisch erzeugt.

Beispiel: Wenn Sie ein Netzwerklaufwerk U: verbunden haben möchten, das je einen Ordner für einen Benutzer enthält, auf das ausschließlich der betreffende Benutzer Zugriff haben soll. Eine solche Verschlüsselungsregel könnte folgendermaßen aussehen:

U:.* <USERKEY>*

Ein weiteres Beispiel für die Anwendung von **<USERKEY>** wäre die Verschlüsselung lokaler temporärer Ordner.

Benutzerspezifische Schlüssel werden in der Standardansicht im Knoten **Zentrale Einstellungen** und dort unter **Alle u.trust LAN Crypt Schlüssel** nicht angezeigt, da sie normalerweise dort nicht benötigt werden. Ein Master Security Officer oder ein Security Officer mit dem globalen Recht **Spezifische Schlüssel verwenden** kann diese Schlüssel jedoch bei Bedarf einblenden, sodass die Daten der einzelnen Schlüssel sichtbar werden.

Im *Eigenschaften*-Dialog des Schlüssels (Kontextmenü / **Eigenschaften**) kann bei Bedarf auch der Schlüsselwert eines spezifischen Schlüssels eingeblendet werden.

Zum Einblenden der spezifischen Schlüssel klicken Sie in der Liste der verfügbaren Schlüssel mit der rechten Maustaste und wählen Sie **Spezifische Schlüssel anzeigen** aus dem Kontextmenü. Es werden dann auch die spezifischen Schlüssel angezeigt. Zum Wechseln in die Standardansicht klicken Sie erneut auf **Spezifische Schlüssel anzeigen**.

Hinweis: Spezifische Schlüssel werden nicht aus der Datenbank entfernt, wenn die dazugehörigen Benutzer/Gruppen gelöscht werden. Sie verbleiben in der Datenbank und können unter dem Knoten **Zentrale Einstellungen** / **Alle u.trust LAN Crypt Schlüssel** über das Kontextmenü **Spezifische Schlüssel anzeigen** angezeigt werden.

Spezifische Schlüssel wieder zuweisen

Es können Situationen auftreten, in denen es notwendig wird, solch einen verwaisten benutzer- bzw. gruppenspezifischen Schlüssel wieder einem Benutzer einer Gruppe zuzuweisen.

Beispiel: Ein Benutzer wird aus dem Active Directory in *u.trust LAN Crypt* importiert. Für diesen Benutzer wird dann ein Benutzerschlüssel angelegt. Wird dann die Gruppe, in der sich der Benutzer befindet, in *u.trust LAN Crypt* komplett gelöscht und später erneut aus einer Verzeichnisdienst-Gruppe oder OU importiert, wird für den Benutzer beim Erzeugen der Profildateien automatisch ein neuer Benutzerschlüssel erzeugt.

Auf Daten, die zuvor mit dem „alten“ Benutzerschlüssel verschlüsselt waren, kann der Benutzer dann nicht mehr zugreifen.

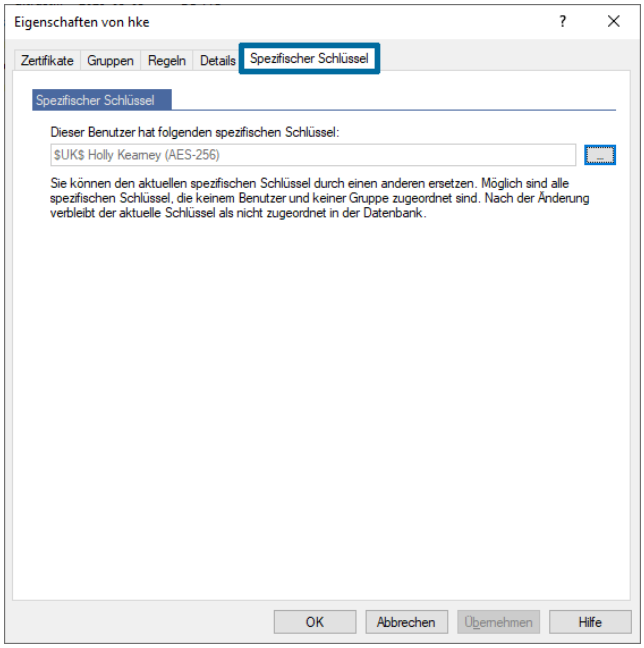
Um solche Situationen zu vermeiden, kann *u.trust LAN Crypt* so konfiguriert werden, dass es möglich ist, die spezifischen Schlüssel von einmal gelöschten Benutzern/Gruppen wieder zuzuweisen.

Fügen Sie hierzu den DWORD-Wert mit dem Namen "ShowUserKeyPage" und dem Wert "1" in der Windows-Registrierung unter dem Schlüssel

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Utimaco\
SGLANCrypt
```

hinzu. Dieser Eintrag in der Registrierung kann auch benutzerspezifisch unter `HKEY_CURRENT_USER\....` eingefügt werden.

Ist dieser Wert in der Windows-Registrierung vorhanden, so wird der Reiter **Spezifischer Schlüssel** dem Dialog *Eigenschaften* von Gruppen und Benutzern hinzugefügt (<Benutzer/Gruppe>/Kontextmenü/Eigenschaften).



In der Ansicht von diesem Reiter können Benutzern/Gruppen in der Datenbank vorhandene nicht zugeordnete spezifische Schlüssel zugeordnet werden.

Ist dem Benutzer/der Gruppe ein spezifischer Schlüssel zugeordnet, wird er im Reiter **Spezifischer Schlüssel** angezeigt. Sie können den aktuellen spezifischen Schlüssel durch einen anderen ersetzen bzw. einen existierenden zuweisen, wenn kein spezifischer Schlüssel angezeigt wird. Zur Verfügung stehen alle spezifischen Schlüssel, die in der Datenbank vorhanden sind und die keinem Benutzer/keiner Gruppe zugeordnet sind.

Hinweis: Ein Security Officer benötigt das globale Recht **Spezifische Schlüssel verwenden**, um an dieser Stelle eine Änderung vornehmen zu können. Besitzt er dieses Recht nicht, hat der Security Officer nur Leserechte.

Durch Klicken auf die **Durchsuchen**-Schaltfläche wird eine Liste aller verfügbaren spezifischen Schlüssel angezeigt. Wählen Sie einen aus und klicken Sie auf **OK**.

Klicken Sie im Reiter **Spezifischer Schlüssel** auf **OK**.

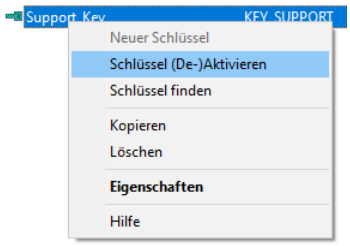
Wurde der aktuelle spezifische Schlüssel durch einen anderen ersetzt, verbleibt er als nicht zugeordneter spezifischer Schlüssel in der Datenbank.

3.15.3 Aktiver / nicht aktiver Schlüssel

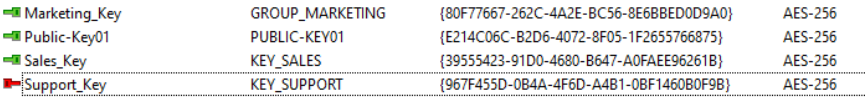
u.trust LAN Crypt bietet die Möglichkeit, bestehende Schlüssel passiv schalten zu können. In der Folge stehen solche Schlüssel bei der Definition von Verschlüsselungsregeln dann nicht mehr zur Verfügung.

In bereits verwendeten Verschlüsselungsregeln können solche Schlüssel weiterverwendet werden. Sie bleiben in der Administrationsdatenbank gespeichert und lassen sich bei Bedarf auch wieder reaktivieren.

Zum Passiv / Aktiv schalten markieren Sie den Schlüssel und klicken Sie im Kontextmenü auf **Schlüssel (De-)Aktivieren**.



Ein rotes Schlüsselsymbol zu Beginn einer Zeile markiert einen passiv geschalteten Schlüssel.



3.15.4 Schlüssel referenzieren

Neben dem Anlegen eines Schlüssels in einer Gruppe können den Benutzern einer Gruppe auch Schlüssel aus einer anderen Gruppe über eine Referenz zur Verfügung gestellt werden.

Beispiel: Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, wenn den Mitgliedern einer Gruppe zeitlich begrenzt Zugriff auf verschlüsselte Daten einer anderen Gruppe gegeben werden soll. Dazu kann der Schlüssel aus einer Gruppe über eine Referenz in die andere Gruppe eingefügt werden und dort zum Erzeugen von Verschlüsselungsregeln für die Daten der anderen Gruppe verwendet werden.

Ohne die Möglichkeit zu referenzieren, müsste zur Realisierung dieses einfachen Datenaustausches eine neue Gruppe angelegt werden, dort die Benutzer beider Gruppen hinzugefügt werden, dann neue Schlüssel und Verschlüsselungsregeln definiert werden. Das Referenzieren stellt eine Möglichkeit dar, den Datenaustausch einfach und schnell zu gestalten.

Um einen Schlüssel einer anderen Gruppe über Referenz hinzuzufügen, ziehen Sie den Knoten **Gruppenschlüssel** einer Gruppe in den Knoten der betreffenden Gruppe. Sie können alternativ den Schlüssel der Quellgruppe auch kopieren und ihn dann in die Zielgruppe einfügen.

Ein Schlüssel, der über eine Referenz eingefügt wurde, wird durch dieses Symbol gekennzeichnet:

Damit ein Security Officer Schlüssel über eine Referenz einfügen darf, muss er über folgende globale Rechte verfügen:

- **Schlüssel erzeugen**
- **Schlüssel kopieren**

Zusätzlich benötigt er in der Quellgruppe die **gruppenspezifischen Rechte**

- **Schlüssel kopieren**

  und

- **Schlüssel erzeugen**

  in der Zielgruppe.

Für das Löschen einer Referenz benötigt er das globale und gruppenspezifische Recht **Schlüssel entfernen**.

Referenzierte Schlüssel haben folgende Eigenschaften:

- Sie werden NICHT vererbt und stehen daher ausschließlich in der Gruppe zur Verfügung, in der sie erzeugt wurden. Sie stehen NICHT in Untergruppen zur Verfügung.
- Wird das „Original“ aus seiner Gruppe entfernt, werden damit auch alle Referenzen entfernt.

Hinweis: Analog zu „normalen“ Gruppenschlüsseln bedeutet das Entfernen einer Referenz nicht, dass die Regel, in der sie verwendet wurde, nicht mehr gültig ist. Damit kein Zugriff auf die Daten (siehe Beispiel) mehr möglich ist, muss die entsprechende Regel gelöscht werden und eine neue Profildatei erzeugt werden. Erst nachdem der Client die neue Profildatei geladen hat, kann er nicht mehr auf die Daten zugreifen.

3.15.5 Schlüssel aus Gruppen entfernen

Das Löschen eines Schlüssels ist nur in der Gruppe möglich, in welcher der Schlüssel erzeugt wurde. Der Schlüssel muss vor dem Löschen deaktiviert werden.

Schlüssel, die in Verwendung sind, werden beim Löschen zwar aus der Gruppe entfernt, verbleiben aber als nicht zugeordnete Schlüssel in der *u.trust LAN Crypt* Datenbank und werden unter dem Knoten **Zentrale Einstellungen / Alle u.trust LAN Crypt Schlüssel** weiterhin angezeigt.

Schlüssel wieder hinzufügen

Sollte ein aus einer Gruppe entfernter Schlüssel später wieder benötigt werden (z. B. zum Zugriff auf ein verschlüsseltes Backup alter Daten), kann er mittels „Drag & Drop“ einfach aus der Liste aller *u.trust LAN Crypt*-Schlüssel auf die betreffende Gruppe gezogen werden und steht dort wieder zur Verfügung. Der Schlüssel kann jeder beliebigen Gruppe, für die der ausführende Security Officer das Recht **Schlüssel erzeugen** hat, hinzugefügt werden. Dabei wird der Schlüssel tatsächlich der Gruppe hinzugefügt, es handelt sich nicht um eine Referenz.

Hinweis: Wird ein Schlüssel entfernt, der nie in einer Regel verwendet wurde, wird er aus der Datenbank gelöscht. Dieser Schlüssel wird dann auch nicht mehr im Knoten **Alle u.trust LAN Crypt Schlüssel** angezeigt.

3.15.6 Schlüssel aus der Datenbank löschen

Unter folgenden Voraussetzungen können Schlüssel im Knoten **Alle u.trust LAN Crypt Schlüssel** tatsächlich aus der Datenbank gelöscht werden:

- Ein Master Security Officer muss angemeldet sein.
- Der Schlüssel darf in keiner Regel verwendet werden.
- Der Schlüssel darf in keiner Gruppe vorhanden sein.
- Der Schlüssel darf kein spezifischer Schlüssel sein, der einem Benutzer oder einer Gruppe zugeordnet ist.
- Der Schlüssel muss deaktiviert sein.

3.15.7 Schlüssel bearbeiten

Der Schlüsselname, die Art der Vererbung und der Kommentar zu einem Schlüssel können geändert werden, nachdem der Schlüssel erzeugt wurde.

Ob ein Schlüssel bereits in Verwendung ist, wird in der Spalte *verwendet* im Schlüsselfenster der Konsole angezeigt.

Zum Ändern eines Schlüssels, wechseln Sie in die Gruppe, in der der Schlüssel erzeugt wurde und klicken Sie doppelt auf den entsprechenden Schlüsselnamen. In diesem Dialog kann der Schlüssel geändert werden.

Der Dialog Eigenschaften

Der Dialog *Eigenschaften* zeigt Informationen zum ausgewählten Schlüssel an. Er ermöglicht die Änderung des langen Schlüsselnamens und der Einstellungen, die die Vererbung des Schlüssels betreffen. Der von *u.trust LAN Crypt* erzeugte 16 Zeichen lange interne Schlüsselname kann nicht geändert werden.

Hinweis: Zum Bearbeiten des Schlüssels muss der Security Officer das gruppenspezifische Recht **Schlüssel erzeugen** in der Gruppe, in der der Schlüssel erzeugt wurde, besitzen. Schlüssel, die in keiner Gruppe vorhanden sind, können nicht bearbeitet werden.

Zur Anzeige der Eigenschaftenseiten eines Schlüssels klicken Sie doppelt auf den Schlüssel.

Der *Eigenschaften* Dialog besteht aus drei Registern:

- Im Register **Schlüssel** werden die Daten des Schlüssels angezeigt. Hier können Sie den langen Schlüsselnamen sowie die Einstellungen, die die Vererbung des Schlüssels betreffen, ändern. Durch Aktivieren der Option **Schlüsselwert anzeigen** kann auch der Schlüsselwert eingeblendet werden.
- Im Register **Gruppen** wird angezeigt, in welchen Gruppen der Schlüssel für Regeln zur Verfügung steht.
- Im Register **Regeln** werden alle Regeln, in denen der Schlüssel verwendet wird, angezeigt.

  Die Register **Gruppen** und **Regeln** dienen nur zu Informationszwecken. Es können dort keine Veränderungen vorgenommen werden.

3.16 Verschlüsselungsregeln

Die *u.trust LAN Crypt* Verschlüsselungsregeln definieren genau, welche Daten mit welchem Schlüssel verschlüsselt werden sollen. Eine Verschlüsselungsregel besteht aus einem Verschlüsselungspfad, einem Dateimuster und einem Schlüssel.

Hinweis: Beachten Sie, dass neben der Pfadangabe für eine Verschlüsselungsregel im darunter liegenden Feld auch das Dateimuster mitanzugeben ist. Sie können hierbei auch Wildcards (z. B. „*.*“) verwenden.

Hinweis: Mit der seit *u.trust LAN Crypt* Version 11.0.0 verfügbaren neuen Funktion „*Multi-Policy-Support*“ wird auch das Laden von mehr als einer Profildatei für Benutzer mithilfe der *u.trust LAN Crypt API* unterstützt. Weitere Informationen hierzu stellen wir Ihnen sehr gerne auf Aufrage zur Verfügung. Wenden Sie sich hierzu bitte an den Utimaco-Support.

Die Verschlüsselungsregeln, die für eine Gruppe definiert werden, bilden ein *u.trust LAN Crypt* Verschlüsselungsprofil.

Das Verschlüsselungsprofil für eine Gruppe kann verschiedene Verschlüsselungsregeln enthalten. Diese können sich auf bestimmte Dateitypen beziehen, die wiederum jeweils mit einem unterschiedlichen Schlüssel und/oder Algorithmus verschlüsselt werden können. Die jeweiligen Dateien oder Dateitypen können sich hierbei sogar im selben Ordner befinden.

Somit besteht die Möglichkeit, ganze Laufwerke, Wechselmedien, optische Laufwerke, Ordner (einschließlich Unterordner), bestimmte Dateitypen (identifiziert durch die Dateiendungen) und einzelne Dateien (identifiziert durch den Dateinamen oder Teilen davon) individuell zu verschlüsseln.

Beim Erzeugen der einzelnen Verschlüsselungsregeln werden alle für die Gruppe vorhandenen Schlüssel angezeigt. Der *u.trust LAN Crypt* Security Officer kann nun durch die Zuweisung der entsprechenden Schlüssel festlegen, auf welche Daten die Benutzer Zugriff haben sollen.

Verschlüsselungsregeln werden immer auf Gruppenbasis erzeugt. Sie bestehen aus einem Pfad, einem Dateimuster sowie einem Schlüssel und werden unter dem Knoten **Verschlüsselungsregeln und Verschlüsselungs-Tags** in den Gruppen (unterhalb des Knotens **Gruppen**) angelegt.

Pfadangabe, Schlüsselauswahl und verschiedene Optionen sind in einem Dialog zusammengefasst, sodass eine Verschlüsselungsregel einfach erzeugt werden kann. Verschlüsselungsregeln können später beliebig verändert werden, z. B., wenn der zuvor gewählte Algorithmus bei einem Schlüssel nicht mehr den geforderten Sicherheitsansprüchen genügen sollte. In dem Fall könnte der bisher verwendete Schlüssel (z. B. mit IDEA-Algorithmus) durch einen neuen Schlüssel mit höherer Sicherheit (z. B. AES-XTS 256 Bit) ersetzt werden. Nach dem Durchführen einer Initialverschlüsselung würden alle vorhandenen Dateien dann mit dem neuen Schlüssel umgeschlüsselt werden.

Hinweis: Verschlüsselungsregeln können grundsätzlich nur in der Gruppe verändert werden, in denen sie auch erzeugt wurden. Ist eine Verschlüsselungsregel „vererbt“, d. h. befindet sie sich in einer Untergruppe, kann sie an dieser Stelle nicht bearbeitet bzw. verändert werden. Sie erkennen dies durch Anzeige einer Gruppe in der Spalte „*Geerbt von*“. In der dort angezeigten Gruppe wurde die Verschlüsselungsregel erzeugt und sie kann auch nur dort verändert werden.

Hinweis: Wenn für eine bestehende Verschlüsselungsregel ein bisher verwendeter Schlüssel durch einen anderen Schlüssel ersetzt werden soll, muss der alte Schlüssel weiterhin in Besitz des Benutzers bleiben. Der alte Schlüssel wird dann für die Umschlüsselung vorhandener verschlüsselter Daten benötigt, die noch mit diesem Schlüssel verschlüsselt sind. Weisen Sie in solchen Fällen den alten Schlüssel als „*Schlüssel ohne Pfad*“ den jeweiligen Benutzern zu.

Hinweis: u.trust empfiehlt grundsätzlich alle Daten nach AES mit einer Schlüssellänge von 256 Bit zu verschlüsseln. Daten, die noch mit einem veralteten Algorithmus (z. B. DES, 3DES, IDEA, XOR) verschlüsselt sind, sollten aus Sicherheitsgründen unbedingt zeitnah nach AES 256 Bit umgeschlüsselt werden.

Verschlüsselungsregeln werden immer an untergeordnete Gruppen vererbt.

Hinweis: Für den Ordner „*Temporäre Internetdateien*“ sollte keine Verschlüsselungsregel definiert werden.

3.16.1 Verschlüsselungspfade

Die Verschlüsselungspfade definieren, welche Daten verschlüsselt werden sollen. Sie definieren diese im Knoten **Verschlüsselungsregeln** *unter dem jeweiligen Gruppenknoten*. Sie gelten dann für alle in dieser Gruppe enthaltenen Benutzer.

Hinweis: Pfade zu „*.zip“-Dateien oder komprimierten Ordnern können nicht als Verschlüsselungspfade verwendet werden.

Hinweis: Bitte beachten Sie, dass Verschlüsselungspfade nicht länger als 259 Zeichen sein dürfen.

Relative Pfade

u.trust LAN Crypt unterstützt relative Pfadangaben. Eine relative Pfadangabe gibt den Pfad zu einem Ordner bzw. einer Datei unabhängig vom Laufwerk bzw. vom übergeordneten Ordner an. Wird eine relative Pfadangabe gewählt, wird jeder Ordner verschlüsselt, auf den die Pfadangabe passt.

Relative Pfade können auf zwei Arten verwendet werden:

- **Eintrag:** `\meine_daten\*.*`

  verschlüsselt alle Root-Ordner, die meine_daten heißen.

  Beispielsweise wären das dann folgende Ordner:

  C:\meine_daten*.*
  D:\meine_daten*.*
  F:\meine_daten*.*
  Z:\meine_daten*.*

- **Eintrag:** `meine_daten\*.*`

  verschlüsselt **ALLE** Ordner, die meine_daten heißen.

  Beispiel:

  C:\firma**meine_daten***.*
  Z:\Abteilung\Buchhaltung\Fibu**meine_daten***.*

In beiden Fällen werden alle Dateien des Ordners „*meine_daten*“ verschlüsselt.

Sobald eine Pfadangabe mit einem Backslash beginnt, bezieht sich die relative Pfadangabe nur noch auf den Root-Bereich.

Standardordner

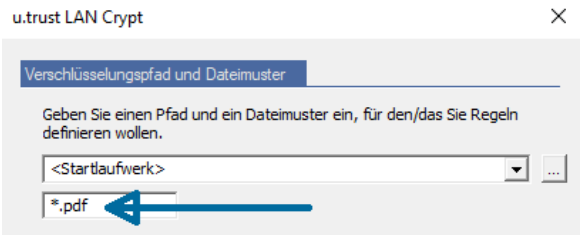
Durch die Unterstützung der von Windows vordefinierten Standardordner, wie beispielsweise *Eigene Dateien*, Gemeinsame Dateien, *Lokale Anwendungsdaten* etc., vereinfacht *u.trust LAN Crypt* die Verschlüsselung dieser benutzerspezifischen Ordner. Die Verwendung der Standardordner befreit den Security Officer somit von der Notwendigkeit, systemspezifische Unterschiede in der Client-Konfiguration zu berücksichtigen. *u.trust LAN Crypt* ermittelt aus dem jeweiligen Standardordner den korrekten benutzerspezifischen Pfad in der richtigen Sprache und verschlüsselt die dort abgelegten Daten.

Startlaufwerk

Durch Auswahl der Option <*Startlaufwerk*> können Sie Dateien, die sich auf dem Systemlaufwerk befinden (dort ist auch Windows installiert), verschlüsseln. Nach Auswahl dieser Option können Sie den vordefinierten Eintrag „*.*“ (dieser gilt für alle Dateien) im Eingabefeld auch anpassen.

Beispiel:

Sollen auf Start- bzw. Systemlaufwerk beispielsweise nur PDF-Dateien verschlüsselt werden, ändern Sie den Eintrag im Eingabefeld für das Dateimuster wie folgt:



Sie können auch noch weitere Dateitypen oder nur ganz bestimmte Dateien (wie beispielsweise „geheim.txt“) auf dem Startlaufwerk verschlüsseln. Hierzu erstellen Sie jeweils eine weitere neue Regel und ändern den Eintrag im Eingabefeld auf die gleiche Weise wie zuvor beschrieben.

Alle lokalen Laufwerke

Mithilfe der Option <*Alle lokalen Laufwerke*> können Sie eine Regel erstellen, die nur für alle lokale Laufwerke gilt. Das könnten beispielsweise (auch mehrere) eingebaute Festplatten, Wechselmedien und auch optische Laufwerke sein.

Optische Laufwerke

Die Option <*Optische Laufwerke*> ermöglicht es, dass Sie eine Regel erstellen können, die ausschließlich für optische Medien gelten soll. Sie können so definieren, dass beispielsweise Daten, die auf eine CD, DVD oder Blue Ray gebrannt werden, immer automatisch von *u.trust LAN Crypt* verschlüsselt werden. Nur Benutzer, die in Besitz des dazugehörigen Schlüssels sind, können diese Daten dann später lesen oder diese miteinander teilen.

Netzwerkfreigaben

Mit Auswahl der Option <*Netzwerkfreigaben*> können Sie eine Regel erstellen, die für alle Netzwerkfreigaben gilt, auf die der Benutzer Zugriff hat. Dabei ist es unerheblich, ob die Netzwerkfreigabe über einen Laufwerksbuchstaben oder aber über einen UNC-Pfad erfolgt.

Wechselmedien

Wenn die Regel nur für Wechselmedien gelten soll, wählen Sie die Option <*Wechselmedien*>. Für Wechselmedien können Sie optional auch noch den Zugriff auf dort gespeicherte Klartext-dateien verweigern (vgl. „*Zugriff auf Klartextdateien für Wechselmedien deaktivieren*“ auf Seite 151).

Hinweis: Beachten Sie, dass unter <*Wechselmedien*> alle extern angeschlossenen Speichermedien (z. B. USB-Sticks, externe Festplatten) zu verstehen sind. Das gilt dann auch für extern angeschlossene optische Laufwerke. Zudem gehören Wechselmedien auch zu den lokalen Laufwerken.

Lokale Festplatten

Sie können durch Auswahl der Option <*Lokale Festplatten*> eine Regel erstellen, die dann für alle lokal eingebauten Festplatten gilt.

Umgebungsvariablen

u.trust LAN Crypt unterstützt die Verwendung der lokalen Umgebungsvariable *%USERNAME%* in Pfadangaben. Die Umgebungsvariable *%USERNAME%* in Pfadangaben wird von *u.trust LAN Crypt* standardmäßig aufgelöst (ausgenommen sind Pfade in *Bypass-Regeln*). Sollen auch noch weitere Umgebungsvariablen aufgelöst werden, muss dies in der *u.trust LAN Crypt*-Konfiguration eingestellt werden (siehe „*Alle Umgebungsvariablen verwenden*“ auf Seite 178).

In dem Fall könnten auch noch weitere Umgebungsvariablen, wie im Folgenden beispielhaft aufgeführt, als Pfadangabe verwendet werden:

Umgebungsvariable:	Beispiel:
%ALLUSERSPROFILE%	C:\ProgramData
%APPDATA%	C:\Users*username*\AppData\Roaming
%LOCALAPPDATA%	C:\Users*username*\AppData\Local
%PUBLIC%	C:\Users\Public
%USERPROFILE%	C:\Users\username

3.16.2 Schlüssel

Die Schlüssel zur Verschlüsselung der Daten werden vor dem Erzeugen der Verschlüsselungsregel angelegt. Alle für die betreffende Gruppe verfügbaren Schlüssel werden im Dialog zum Erstellen einer Verschlüsselungsregel angezeigt und können aus einer Liste ausgewählt werden.

3.16.3 Reihenfolge der Verschlüsselungsregeln

u.trust LAN Crypt sortiert die Verschlüsselungsregeln beim Laden der Profildateien auf dem Client nach der Methode, die Sie im Reiter **Regeln auflösen** im Knoten **Zentrale Einstellungen** in der *u.trust LAN Crypt* Administration ausgewählt haben (siehe “Sortiermethoden“ auf Seite 54).

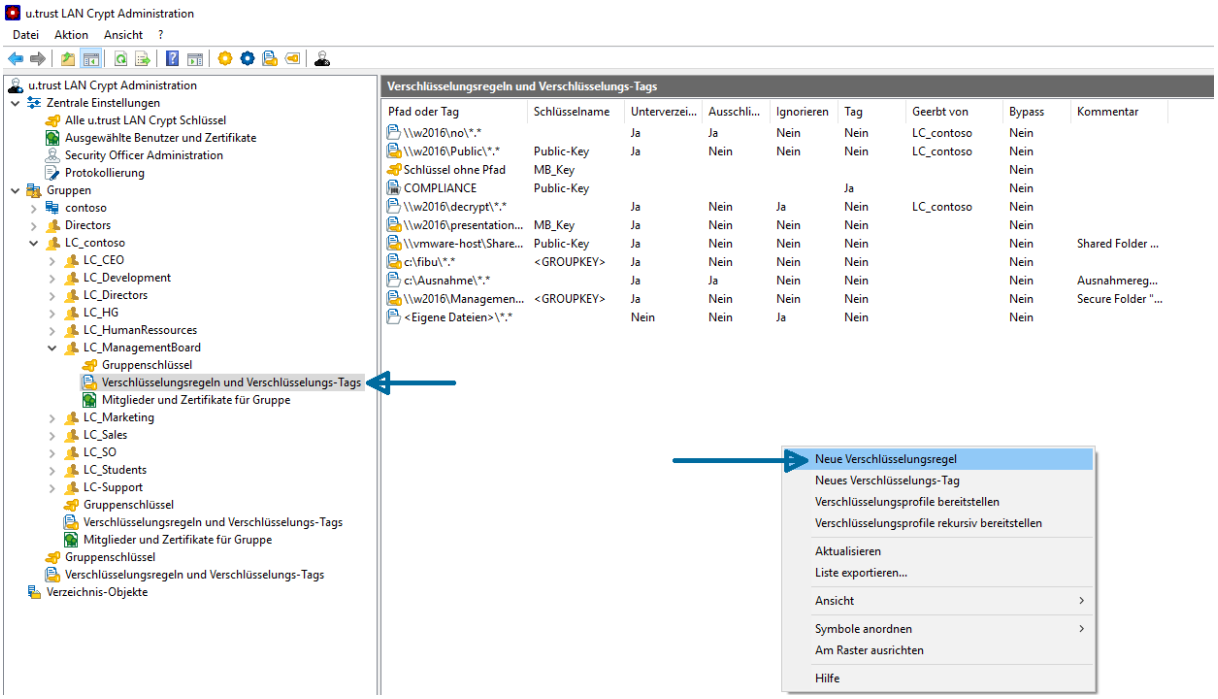
3.16.4 Erzeugen von Verschlüsselungsregeln

1. Wählen Sie aus dem Knoten **Gruppen** die Gruppe aus, für die Sie eine Verschlüsselungsregel erstellen wollen.

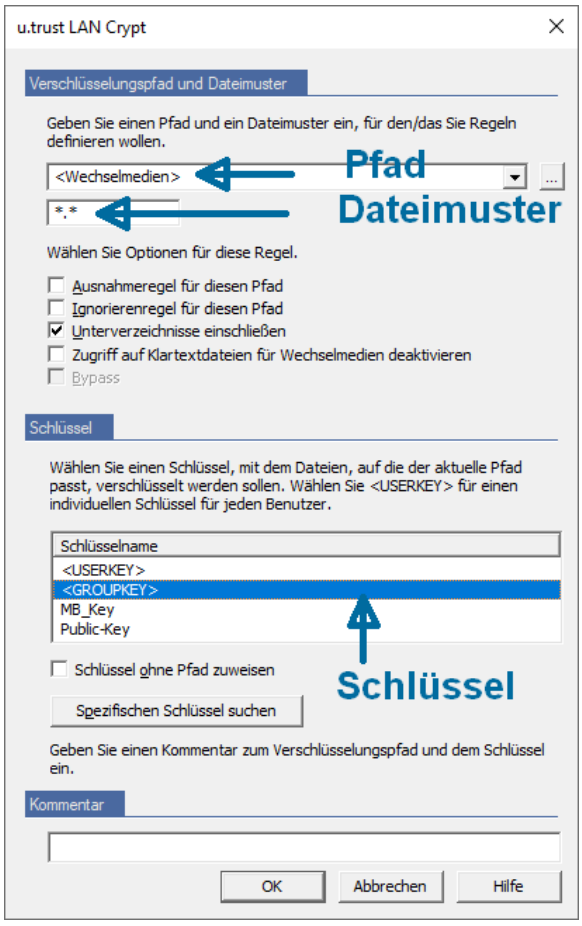
   Hinweis: Mithilfe der Funktion **Finde Gruppe** können Sie auch nach einer bestimmten Gruppe suchen (siehe Abschnitt 3.10.6 „*Finde Gruppe*“ auf Seite 116).

2. Klicken Sie mit der rechten Maustaste auf **Verschlüsselungsregeln und Verschlüsselungs-Tags** unterhalb des jeweiligen Gruppenknotens und klicken Sie auf **Neue Verschlüsselungsregel** im Kontextmenü.

Wurden bereits Regeln erzeugt, werden diese im rechten Konsolenfenster angezeigt.



Der Befehl **Neue Verschlüsselungsregel** steht auch über ein Kontextmenü zur Verfügung, wenn Sie im rechten Konsolenfenster mit der rechten Maustaste klicken.



3. Geben Sie im Eingabefeld unter *Verschlüsselungspfad und Dateimuster* einen relativen oder absoluten Pfad ein.

4. Wenn die neue Verschlüsselungsregel alle Dateien im gewählten Pfad betreffen soll, geben Sie in das darunter liegende Eingabefeld „*.*“ als Dateimuster ein. Soll die neue Regel dagegen nur für bestimmte Dateitypen gelten, geben Sie dort als Dateimuster beispielsweise „*.*docx*“ (für Worddateien) oder „*.txt (für Textdateien) ein. Die Verwendung von Jokern (?) und Wildcards (*) in Dateinamen (nicht jedoch im restlichen Pfad) ist erlaubt (z. B. „*.*d??*“ oder auch „*.*d**“). Klicken Sie ggf. auf **Durchsuchen** ("..."), wenn Sie für die Regel einen bestimmten Pfad über den Dateiexplorer auswählen möchten.

   Alternativ können Sie auch einen der im Listenfeld enthaltenen vordefinierten Pfade von Windows-Standardordnern (z. B. *Eigene Dateien* etc.), bestimmte Laufwerke, Netzwerkfreigaben oder Laufwerkstypen (z. B. *Wechselmedien*, *optische Laufwerke* etc.) wählen. Der entsprechend gewählte vordefinierte Pfad wird dann im Eingabefeld anzeigt.

   Folgende vordefinierte Pfade können für die Verschlüsselungsregel gewählt werden:

   ```
   <Lokale Anwendungsdaten>
   <Anwendungsdaten>
   <Gemeinsame Anwendungsdaten>
   <Eigene Dateien>
   <Gemeinsame Dateien>
   <Internet Cache>
   <Startlaufwerk>
   <Alle lokalen Laufwerke>
   <Optische Laufwerke>
   <Netzwerkfreigaben>
   <Wechselmedien>
   <Lokale Festplatten>
   ```

   Auch hier können Sie die vordefinierte Angabe des Dateimusters „*.*“ wie bereits zuvor beschrieben individuell anpassen. Ergänzende Informationen zu den vordefinierten Pfaden finden Sie am Anfang dieses Abschnitts ab Seite 143.

Relative Pfade und Programme, die ausschließlich Datei- bzw. Pfadangaben in 8.3 Notation beherrschen

Bei der Verwendung von Programmen, die ausschließlich Datei- bzw. Pfadangaben in 8.3 Notation beherrschen und die auf verschlüsselte Dateien mit Dateinamen länger als 8 Zeichen oder auf Dateien in Ordnern mit Namen länger als 8 Zeichen zugreifen, müssen relative Verschlüsselungspfade in 8.3 Notation angegeben werden.

Diese Verschlüsselungsregeln müssen zusätzlich definiert werden. Andernfalls werden 32-Bit-Programme nicht mehr funktionieren.

Das Kommando dir /x kann zur Anzeige des korrekten 8.3-Namens von langen Dateinamen verwendet werden.

5. Unter *Verschlüsselungspfad und Dateimuster* werden bis zu fünf Optionen angezeigt:
   - Unterverzeichnisse einschließen
   - Ausnahmeregel für diesen Pfad
   - Ignorierenregel für diesen Pfad
   - Zugriff auf Klartextdateien für Wechselmedien deaktivieren
   - Bypass

Unterverzeichnisse einschließen

Wenn nicht ausdrücklich angegeben, werden Unterverzeichnisse bzw. Unterordner nicht in die Regel einbezogen. Wenn die Regel (z B. eine Verschlüsselungsregel) auch für diese gelten soll, muss die Option **Unterverzeichnisse einschließen** aktiviert werden.

Beispiel:

Eintrag: `c:\unternehmen\meine_daten\*.*` Unterverzeichnisse einschließen

Diese Verschlüsselungsregel verschlüsselt alle Dateien in:

C:\unternehmen\meine_daten

C:\unternehmen\meine_daten\projekt X

C:\unternehmen\meine_daten\projekt X\demo

Ausnahmeregel für diesen Pfad

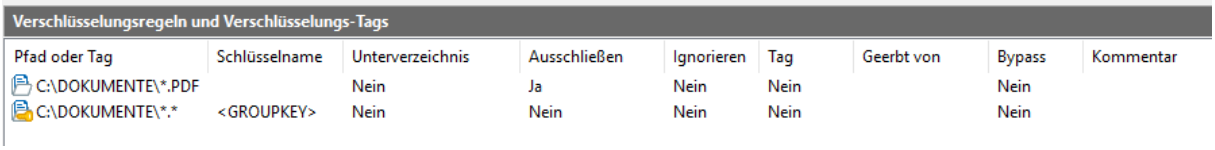
Diese Option kann in einer Verschlüsselungsregel genutzt werden, um einzelne Dateien, Dateitypen oder Unterordner eines Pfades, für den bereits eine Verschlüsselungsregel besteht, von der Verschlüsselung auszuschließen. Dies wird erreicht, indem Sie die Option **Ausnahmeregel für diesen Pfad** im Dialog *Neue Verschlüsselungsregel* aktivieren. Damit werden die in der Verschlüsselungsregel angegebenen Dateien nicht verschlüsselt. Sie können dies auch bei bereits vorhandenen Verschlüsselungsregeln ändern, indem Sie eine vorhandene Regel mit doppeltem Mausklick oder über das Kontextmenü *Eigenschaften* auswählen.

Sie können eine solche Regel ebenfalls für bereits vordefinierte Laufwerkstypen, Laufwerke, bestimmte Ordner, Dateitypen oder Dateien definieren.

Die Pfadangaben erfolgen an dieser Stelle analog zu den Pfadangaben von Verschlüsselungsregeln (vgl. „*Erzeugen von Verschlüsselungsregeln*“ ab Seite 145).

Beispiel:

Alle Dateien mit der Dateierweiterung „*.PDF*“ sollen von der Verschlüsselung im Ordner *C:\DOKUMENTE* ausgeschlossen werden.



Erste Zeile:

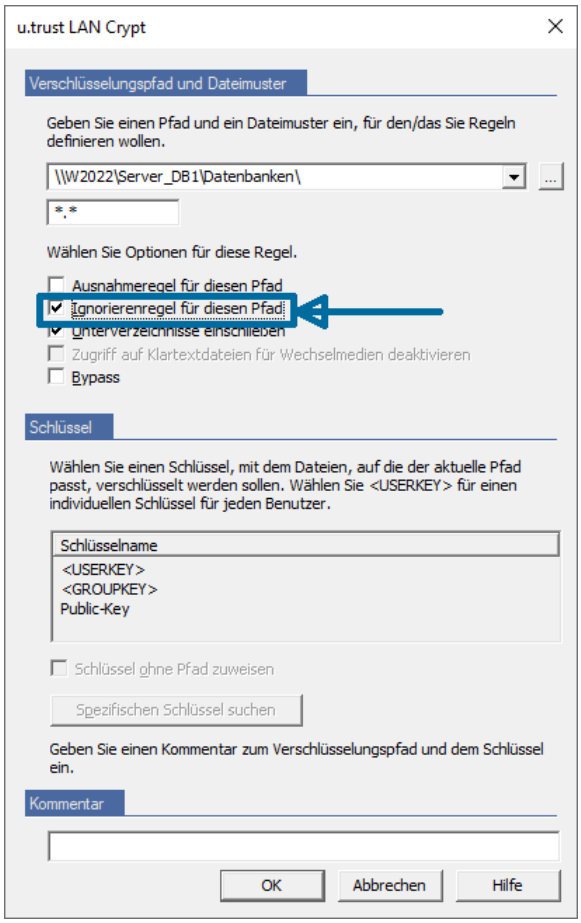
Pfadeintrag C:\DOKUMENTE und Dateimuster *.PDF, **Ausnahmeregel für diesen Pfad** aktiviert bzw. markiert und kein Schlüssel ausgewählt: schließt alle Dateien mit der Erweiterung „*.PDF*“ im Ordner C:\DOKUMENTE von der Verschlüsselung aus.

Zweite Zeile:

Pfadeintrag C:\DOKUMENTE und Dateimuster *.*, **Ausnahmeregel für diesen Pfad** nicht markiert und ein Schlüssel ausgewählt, verschlüsselt alle Dateien im Ordner C:\DOKUMENTE (außer „.PDF“, da in Zeile 1 ausgeschlossen) mit dem angegebenen Schlüssel.

Ignorierenregel für diesen Pfad

u.trust LAN Crypt bietet die Option **Ignorierenregel für diesen Pfad** an. Dateien, die hiervon betroffen sind, werden von *u.trust LAN Crypt* vollständig ignoriert und nicht verschlüsselt.



Sie können eine solche Regel ebenfalls für bereits vordefinierte Laufwerkstypen, Laufwerke, bestimmte Ordner, Dateitypen oder Dateien definieren.

Die Pfadangaben erfolgen an dieser Stelle analog zu den Pfadangaben von Verschlüsselungsregeln (vgl. „*Erzeugen von Verschlüsselungsregeln*“ ab Seite 145).

Sie können hierbei jeweils über das Dateimuster definieren, ob an diesen Speicherorten alle (*.*), nur bestimmte Dateitypen (beispielsweise *.exe für Anwendungen) oder individuelle Dateien von *u.trust LAN Crypt* ignoriert werden sollen.

Alternativ können Sie aber weiterhin auch jeden anderen beliebigen Pfad wählen.

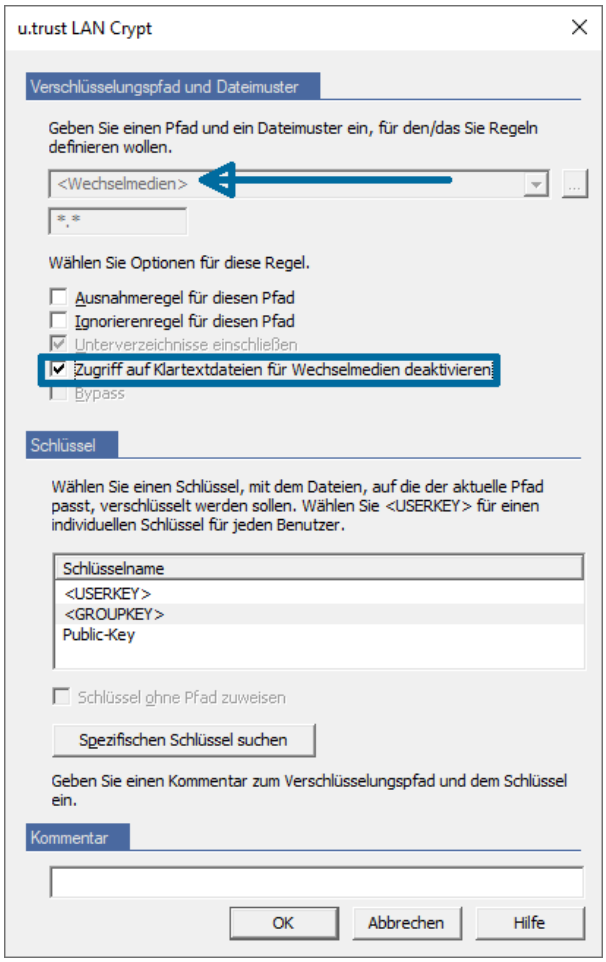
Wenn Sie die Option **Ignorierenregel für diesen Pfad** gesetzt haben, heißt das, dass für Dateien, die von dieser Regel betroffen sind, auch kein Zugriffsschutz durch *u.trust LAN Crypt* besteht. Dateien in diesen Pfaden können beliebig von jedermann geöffnet (ein ggf. verschlüsselter Inhalt einer Datei wird verschlüsselt angezeigt), verschoben, gelöscht usw. werden. Für Dateien in Ordnern, für die dagegen eine **Ausnahmeregel für diesen Pfad** besteht, werden jedoch von *u.trust LAN Crypt* überprüft, ob sie verschlüsselt sind oder nicht. Ein Zugriff auf verschlüsselte Dateien wird dann dem Benutzer verwehrt, wenn dieser nicht im Besitz des hierfür erforderlichen Schlüssels ist.

Hinweis: Wir möchten an dieser Stelle darauf hinweisen, dass sich an dieser Stelle Legacy- und Minifiltertreiber beim *u.trust LAN Crypt* Client teilweise unterschiedlich verhalten. Während bei aktiviertem Minifiltertreiber die Regel **Ignorierenregel für diesen Pfad** bewirkt, dass dort auch der Zugriffsschutz für die hiervon betroffenen Dateien deaktiviert ist, bleibt dieser dagegen bei aktiviertem Legacyfiltertreiber (ältere *u.trust LAN Crypt Clients*) bestehen.

Die Option **Ignorierenregel für diesen Pfad** wird hauptsächlich für Dateien verwendet, auf die sehr häufig zugegriffen wird und für die es keine Veranlassung gibt, sie zu verschlüsseln. Auf diese Weise lässt sich die System-Leistung steigern. Auch der Installationsort von *u.trust LAN Crypt* oder auch der von Windows selbst wird von der Verschlüsselung ignoriert. Es lassen sich grundsätzlich keine Dateien ver- oder entschlüsseln, wenn für diese eine **Ignorierenregel für diesen Pfad** besteht. Solche Dateien werden von *u.trust LAN Crypt* komplett ignoriert.

Zugriff auf Klartextdateien für Wechselmedien deaktivieren

Diese Option steht nur für Verschlüsselungsregeln zur Verfügung, bei denen <*Wechselmedien*> als vordefinierter Pfad gewählt ist. Wenn Sie die Option **Zugriff auf Klartextdateien für Wechselmedien deaktivieren** gesetzt haben, wird auf Wechselmedien (wie z. B. für externe Festplatten, USB-Sticks etc.), für die eine solche Verschlüsselungsregel besteht, der Zugriff auf dort ggf. vorhandene unverschlüsselte Dateien (Klartextdateien) verweigert. Benutzer können auf Wechselmedien dann Klartextdateien weder öffnen noch lesen.



Mit dem Setzen der Option **Zugriff auf Klartextdateien für Wechselmedien deaktivieren** können Sie u. a. verhindern, dass von Wechselmedien, wie z. B. USB-Sticks, unerwünschte Software installiert wird.

Hinweis: Sobald Sie diese Option aktivieren, hat das unmittelbar zur Folge, dass automatisch auch die Option **Unterverzeichnisse einschließen** für die Verschlüsselungsregel gesetzt wird.

Hinweis: Sie müssen dieser Verschlüsselungsregel einen Schlüssel zuweisen.

Bypass-Regel setzen

u.trust LAN Crypt bietet als Regel die Option **Bypass** an. Alle Pfade, für die eine solche Regel besteht, werden durch den *u.trust LAN Crypt* Minifiltertreiber vollständig ignoriert. Dateien, die sich in solchen Pfaden befinden, können dort weder ver- noch entschlüsselt werden. Im Vergleich mit der Option **Ignorierenregel für diesen Pfad** werden in Pfaden, für die eine *Bypass-Regel* gilt, auch Dateizugriffe nicht mehr durch den Minifiltertreiber überwacht.

Hinweis: Sobald Sie diese Option aktivieren, hat das unmittelbar zur Folge, dass automatisch auch die Option **Unterverzeichnisse einschließen** für diese Regel gesetzt wird.

Hinweis: Für Pfadangaben in *Bypass-Regeln* können keine Umgebungsvariablen verwendet werden.

Hinweis: Pfadangaben in *Bypass-Regeln* dürfen keine Laufwerksbuchstaben enthalten.

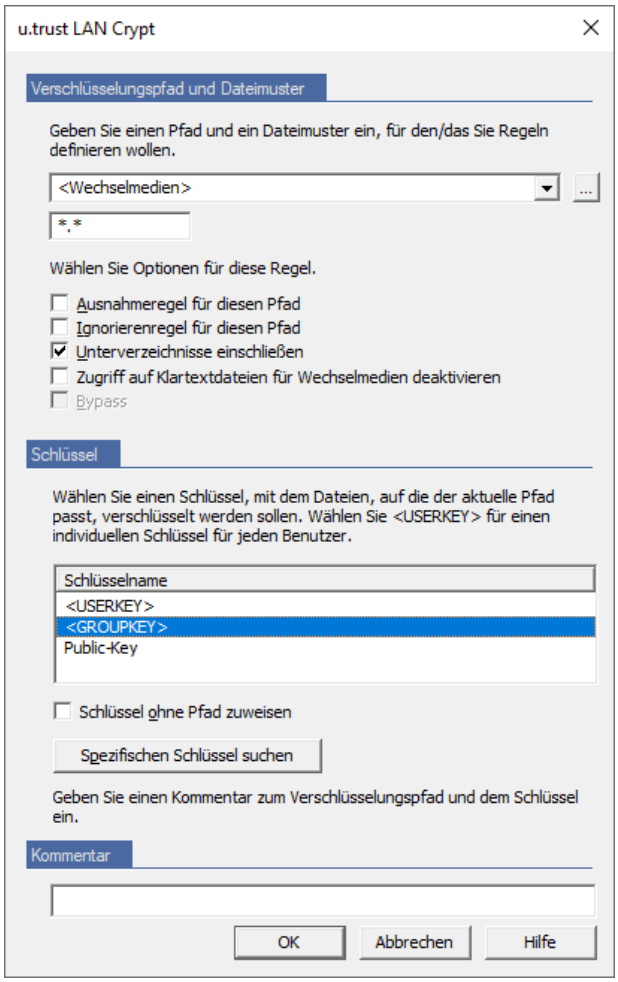
Achtung: Aktivieren Sie diese Option grundsätzlich nur dann, wenn ein Utimaco Support-Mitarbeiter Sie hierzu aufgefordert hat!

Hinweis: Nach dem Setzen oder Entfernen einer *Bypass-Regel* müssen Sie den Client-Rechner neu starten.

Hinweis: Diese Funktion ist nur verfügbar, wenn Sie diese im Knoten **Zentrale Einstellungen**, im Reiter **Regeln auflösen** aktiviert haben (siehe „Administration ist Besitzer für Bypass-Regeln in der Registry“ auf Seite 58).

Wenn Sie eine Verschlüsselungsregel mit Schlüssel erstellen wollen, führen Sie die folgenden weiteren Schritte aus:

6. Wählen Sie einen Schlüssel aus der Liste *Schlüsselname* aus.



Hinweis: In der Standardansicht werden nur die Platzhalter für *<USERKEY>* und *<GROUPKEY>* sowie die von einem (Master) Security Officer erzeugten Schlüssel angezeigt. Durch Klicken auf die Schaltfläche **Spezifischen Schlüssel suchen** können Sie auch nach spezifischen Schlüsseln (wie z. B. derzeit nicht zugewiesene Schlüssel) suchen und sich diese anzeigen lassen.

Verschlüsselungspfad und Schlüssel bilden eine *u.trust LAN Crypt*-Verschlüsselungsregel. Die Gesamtheit der Verschlüsselungsregeln, die Sie für den Benutzer/die Gruppe definieren, bildet das Verschlüsselungsprofil des Benutzers/der Gruppe.

<USERKEY>

In der Liste der Schlüssel wird auch immer ein Schlüssel *<USERKEY>* angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.

<GROUPKEY>

Analog zur Verwendung von *<USERKEY>* kann durch die Verwendung von *<GROUPKEY>* ein gruppenspezifischer Schlüssel für alle Mitglieder der Gruppe erzeugt werden.

Hinweis: Stellen Sie bei der Verwendung von <*USERKEY*> sicher, dass ausschließlich der Benutzer, dem dieser Schlüssel zugewiesen wurde, auf die Daten zugreift. Andere Benutzer können diese Daten nicht entschlüsseln!

Beispiel: Ein Beispiel für die Anwendung von <*USERKEY*> wäre, wenn alle Benutzer z. B. über ein Netzwerklaufwerk `U:` verbunden sind, das je einen Ordner für einen Benutzer enthält. Ausschließlich der betreffende Benutzer soll darauf Zugriff haben.

Eine solche Verschlüsselungsregel könnte folgendermaßen aussehen:

```
U:\*.* <USERKEY>
```

Ein weiteres Beispiel für die Anwendung von <*USERKEY*> wäre die Verschlüsselung von lokalen temporären Ordnern bzw. Verzeichnissen.

Schlüssel ohne Pfad

In der Liste der definierten Verschlüsselungspfade befindet sich auch ein Platzhalter *Schlüssel ohne Pfad*.

Er dient dazu, dem Benutzer einen Schlüssel zur Verfügung zu stellen, mit dem er auf verschlüsselte Daten zugreifen kann, für die keine Verschlüsselungsregel existiert. Dies kann der Fall sein, wenn verschlüsselte Dateien an einen Ort kopiert werden (bei deaktivierter Verschlüsselung), für den keine Verschlüsselungsregel definiert wurde. Der Zugriff auf diese Dateien ist mit dem entsprechenden Schlüssel weiter möglich. Ein *Schlüssel ohne Pfad* wird meist auch zur Umschlüsselung von Daten benötigt, und zwar immer dann, wenn für diesen (alten) Schlüssel keine Verschlüsselungsregel mehr besteht (siehe hierzu auch den Hinweis im Abschnitt „Verschlüsselungsregeln“ auf Seite 142).

Wird ein Schlüssel ohne Pfad angelegt, wird automatisch ein neuer Platzhalter angelegt, um die Erzeugung weiterer Schlüssel ohne Pfad zu ermöglichen.

7. Markieren Sie die entsprechenden Optionen.
8. Unter *Kommentar* können Sie eine Beschreibung oder Informationen über die angelegte Verschlüsselungsregel eingeben.
9. Klicken Sie auf **OK**.

Die neue Verschlüsselungsregel wird in der *u.trust LAN Crypt* Administration angezeigt.

Zum Bearbeiten bestehender Verschlüsselungsregeln markieren Sie diese und klicken Sie auf **Eigenschaften** im *Kontextmenü*. Oder doppelklicken Sie den entsprechenden Eintrag.

Hinweis: Verschlüsselungsregeln können grundsätzlich nur in den Gruppen verändert werden, in denen sie auch erzeugt wurden.

3.16.5 Suchen eines spezifischen Schlüssels

Klicken Sie auf die Schaltfläche **Spezifischer Schlüssel**, um einen Assistenten für die Suche nach spezifischen Schlüsseln zu starten. Schlüssel, die im Assistenten ausgewählt werden, werden zur Schlüsselliste hinzugefügt und können für Verschlüsselungsregeln benutzt werden. Der Schlüssel wird nur vorübergehend hinzugefügt. Wird der Assistent erneut ausgeführt und ein anderer Schlüssel ausgewählt, so wird der zuvor hinzugefügte Schlüssel aus der Liste entfernt.

Auf der ersten Seite können Sie Suchkriterien festlegen. Folgende Kriterien stehen in der Dropdown-Liste zur Auswahl:

- **Einem Benutzer zugewiesener Schlüssel**

  Sucht nach allen spezifischen Schlüsseln, die einem Benutzer zugewiesen sind. Geben Sie den Benutzernamen oder den Anmeldenamen im Eingabefeld (Suchbedingung) ein. Für Platzhaltersuchvorgänge können Sie SQL-Platzhalter verwenden. Wenn Sie zum Beispiel "Vorstand Benutzer 1%" eingeben, werden alle Schlüssel gefunden, die Benutzern zugewiesen sind, deren Benutzer- oder Anmeldenamen mit "Vorstand Benutzer 1" beginnen.

- **Einer Gruppe zugewiesener Schlüssel**

  Sucht nach allen spezifischen Schlüsseln, die einer Gruppe zugewiesen sind. Geben Sie den Namen der Gruppe ein.

- **Schlüsselname**

  Sucht nach allen spezifischen Schlüsseln mit einem bestimmten Namen. Geben Sie den langen oder den kurzen Namen des Schlüssels ein.

- **Schlüssel-GUID**

  Sucht nach allen spezifischen Schlüsseln mit einer bestimmten GUID. Geben Sie die GUID des Schlüssels ein.

- **Zurzeit nicht zugewiesene Schlüssel**

  Zeigt alle Schlüssel, die derzeit keinem Benutzer und keiner Gruppe zugewiesen sind.

Das Suchergebnis wird auf der zweiten Seite angezeigt.

Wenn ein Schlüssel derzeit zugewiesen ist, wird der Benutzer- oder der Gruppenname unter der Spalte **Zugewiesen an** angezeigt. Die Liste enthält nur spezifische Schlüssel, auch wenn nicht-spezifische Schlüssel die Suchkriterien erfüllen würden.

Wählen Sie einen Schlüssel aus und klicken Sie auf **Beenden**, um den Schlüssel zur Liste im Dialog für das Erstellen von Verschlüsselungsregeln hinzuzufügen.

3.17 Verschlüsselungs-Tags

Identifiziert ein DLP-Produkt Daten, die verschlüsselt werden sollen, so kann es die *u.trust LAN Crypt Client*-API verwenden, um die Dateien zu verschlüsseln. In der *u.trust LAN Crypt* Administration können Sie unterschiedliche Verschlüsselungs-Tags definieren, die den zu verwendenden *u.trust LAN Crypt*-Schlüssel angeben.

Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden wie z. B. das Verschlüsselungs-Tag <*CONFIDENTIAL*>, um alle Dateien zu verschlüsseln, die als vertraulich von Ihrem DLP-Produkt kategorisiert sind.

Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre:

```
SGFEAPI encrypt /Tag:CONFIDENTIAL c:\Dokumente\geheim.docx
```

Damit würde die Datei *geheim.docx* im Ordner *\Dokumente* mit dem Schlüssel aus dem Verschlüsselungs-Tag <*CONFIDENTIAL*> verschlüsselt.

Um ein Verschlüsselungs-Tag zu erzeugen

1. klicken Sie mit der rechten Maustaste auf **Verschlüsselungsregeln und Verschlüsselungs-Tags** unter dem entsprechenden Gruppenknoten, und klicken Sie auf **Neues Verschlüsselungs-Tag** im Kontextmenü.

   Der Befehl **Neues Verschlüsselungs-Tag** steht auch über ein Kontextmenü zur Verfügung, wenn Sie im rechten Konsolenfenster mit der rechten Maustaste klicken. Im rechten Konsolenfenster werden alle erzeugten Verschlüsselungsregeln und Verschlüsselungs-Tags angezeigt.

2. Geben Sie in das Eingabefeld unter *Verschlüsselungs-Tag* eine schlüssige Bezeichnung ein, wie z. B. <*CONFIDENTIAL*> und klicken Sie auf **OK**.

3. Wählen Sie einen Schlüssel aus.

Weitere Details hierzu finden Sie in der Client-API-Dokumentation im Ordner *\api* Ihres entpackten Installationspaketes.

Hinweis: In der Standardansicht werden nur die Platzhalter für <*USERKEY*> und <*GROUPKEY*> sowie die von einem Security Officer erzeugten Schlüssel angezeigt. Über die Schaltfläche **Spezifischen Schlüssel suchen**, können Sie auch nach spezifischen Schlüsseln suchen und sich diese anzeigen lassen (siehe Kapitel zuvor).

<USERKEY>

In der Liste der Schlüssel wird auch immer ein Schlüssel <*USERKEY*> angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.

<GROUPKEY>

Analog zur Verwendung von <*USERKEY*> kann durch die Verwendung von <*GROUPKEY*> ein gruppenspezifischer Schlüssel für alle Mitglieder der Gruppe erzeugt werden.

Hinweis: Stellen Sie bei der Verwendung von <USERKEY> sicher, dass ausschließlich der Benutzer, dem dieser Schlüssel zugewiesen wurde, auf die Daten zugreift. Andere Benutzer können diese Daten nicht entschlüsseln!

4. Unter Kommentar können Sie eine Beschreibung oder Informationen über die angelegte Verschlüsselungsregel eingeben.

5. Klicken Sie auf **OK**.

Das neue Verschlüsselungs-Tag wird in der *u.trust LAN Crypt* Administration angezeigt.

Zum Bearbeiten bestehender Verschlüsselungs-Tags markieren Sie diese und klicken Sie auf **Eigenschaften** im Kontextmenü. Oder doppelklicken Sie auf den entsprechenden Eintrag.

3.18 Zuordnung der Zertifikate

Jedes Profil ist mit dem öffentlichen Schlüssel seines Benutzers geschützt. Über die *u.trust LAN Crypt* Administration wird jedem Benutzer eine Schlüsseldatei (**.p12-Datei*) zugewiesen. Diese enthält neben dem Zertifikat auch den privaten Schlüssel. Der private Schlüssel wird mittels PIN vor unautorisiertem Zugriff geschützt. *u.trust LAN Crypt* schreibt die dazugehörige PIN in die Passwortprotokolldatei (*p12pwlog.csv*). Diese Datei sollte vor unberechtigten Zugriffen immer besonders geschützt werden. Um das zu realisieren, könnte beispielsweise der Security Officer auf dem *u.trust LAN Crypt* Admin-Computer auch die *u.trust LAN Crypt* Client-Anwendung installieren und eine Verschlüsselungsregel für die Passwortprotokolldatei erstellen.

Hinweis: Wenn Sie beide *u.trust LAN Crypt* Komponenten, *Admin-Konsole* und *Client-Anwendung* auf demselben Computer installieren, **müssen diese immer von der gleichen Version** sein.

Alternativ können Sie Zertifikate auch von einer PKI verwenden. Es ist empfehlenswert, dass die Zertifikate bereits im Zertifikatsspeicher bzw. in einem Ordner zur Verfügung stehen (z. B. LDAP), wenn Sie mit der Zuweisung beginnen. Zum Importieren der Zertifikate in den entsprechenden Zertifikatsspeicher können die Windows Standardmechanismen verwendet werden.

Zur automatischen Zuordnung der Zertifikate stellt *u.trust LAN Crypt* einen Zertifikats-zuordnungsassistenten zur Verfügung.

Hinweis: Wenn der Security Officer, der die Zertifikatszuordnung durchführt, im Dateisystem kein Recht hat, die Passwortprotokolldatei zu ändern, können keine *u.trust LAN Crypt*-Zertifikate erzeugt werden.

3.18.1 Zertifikat einem Benutzer zuordnen

Zum Zuweisen eines Zertifikats

1. Markieren Sie **Mitglieder und Zertifikate für Gruppe** unter dem jeweiligen Gruppenknoten. Im rechten Konsolenfeld werden alle Benutzer aufgelistet.

2. Klicken Sie doppelt auf einen Benutzer oder klicken Sie mit der rechten Maustaste auf den Benutzer und anschließend auf dessen **Eigenschaften** im Kontextmenü. Der Dialog *Eigenschaften von ...* wird angezeigt.

3. Der Dialog bietet folgende Möglichkeiten, dem Benutzer ein oder mehrere Zertifikate zuzuweisen:

   - **Neu**

     Dem Benutzer kann hiermit ein neues Zertifikat zugewiesen werden. Sollten keine Zertifikate zur Verfügung stehen, kann die Administration von *u.trust LAN Crypt* optional selbst Zertifikate erzeugen. Diese Zertifikate sollten ausschließlich von *u.trust LAN Crypt* verwendet werden!

     Das erzeugte Zertifikat wird als *PKCS#12-Datei* im vordefinierten Ordner gespeichert (siehe Reiter **Verzeichnisse** im Knoten **Zentrale Einstellungen**).

     Hinweis: Die so erzeugten Zertifikate müssen anschließend an die jeweiligen Benutzer verteilt werden. Andernfalls haben die Benutzer keinen Zugriff auf ihre Verschlüsselungsprofile.

   - **Importieren**

     Sollte das gewünschte Zertifikat noch nicht im Zertifikatsspeicher vorhanden sein, wird es in der Liste der verfügbaren Zertifikate nicht angezeigt.

     Klicken Sie in diesem Fall auf **Importieren.** Es wird ein Dialog geöffnet, in dem Sie das gewünschte Zertifikat über einen Pfad auswählen können. Klicken Sie anschließend auf **OK** und das Zertifikat wird dem Benutzer zugeordnet.

     Hinweis: Es können hierbei nur X.509-Zertifikatsdateien in den Formaten „**.cer*“, „**.crt*“ und „**.der*“ importiert werden, jedoch nicht „**.p12*“- bzw. „**.pfx*“-Dateien.

   - **Hinzufügen**

     Wählen Sie die Quelle für das Zertifikat aus:

     Zertifikat aus dem Zertifikatsspeicher hinzufügen

     Öffnet einen Dialog, in dem ein bestehendes Zertifikat dem Benutzer zugeordnet werden kann. In diesem Dialog werden alle im Zertifikatsspeicher vorhandenen Zertifikate aufgelistet.

     Zertifikate über eine LDAP-Quelle zuordnen

     u.trust LAN Crypt bietet zusätzlich die Möglichkeit, Zertifikate aus einer LDAP-Quelle zuzuweisen.

Wählen Sie die Quelle für das Zertifikat. Markieren Sie hierfür **LDAP** in der Drop-Down-Liste des Dialoges.

Es wird jetzt ein Eingabefeld angezeigt, in das Sie die URL der LDAP-Quelle eingeben können. Nach Klicken auf **Aktualisieren** wird der Inhalt der LDAP-Quelle angezeigt.

Begriffe in eckigen Klammern (z. B. *[Sub_OU1]* bezeichnen die OUs in der LDAP-Quelle. Ein Doppelklick auf eine OU zeigt die darin enthaltenen Zertifikate an.

Ein Doppelklick auf [..] bringt Sie in der Organisationsstruktur eine Ebene höher.

Wählen Sie ein Zertifikat aus und klicken Sie auf **OK**. Das öffentliche Zertifikat wird dann dem Security Officer zugewiesen.

Hinweis: Wenn auf den LDAP-Server nicht über eine Anonymous-Anmeldung zugegriffen werden kann, müssen die Anmeldedaten als Distinguished Name (Beispiel: CN= Max Mustermann,OU=Marketing) im Register **Server** im Knoten **Zentrale Einstellungen** erfolgen.

Hinweis: Wenn das Zertifikat aus einem LDAP-Verzeichnis zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Benutzers vorhanden sein.

4. Wählen Sie durch eine der Möglichkeiten ein Zertifikat aus und klicken Sie auf **OK**.

Im Konsolenfenster rechts neben dem Benutzer werden nun Informationen über das verwendete Zertifikat angezeigt (Gültigkeitsdauer, Seriennummer, Antragsteller, Aussteller).

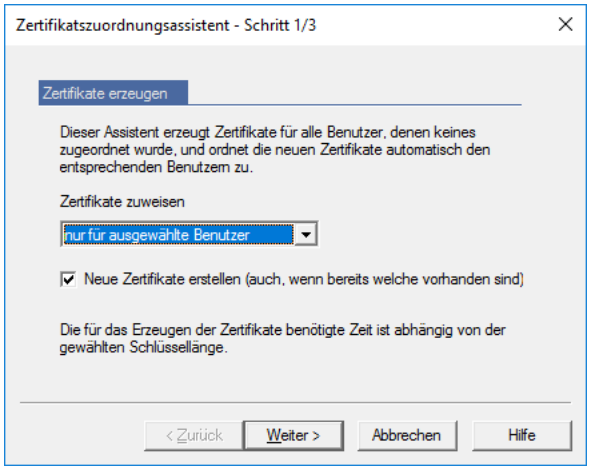
Hinweis: Das Zertifikats-Snap-In steht unter jedem Benutzer-/Gruppen-Knoten zur Verfügung. Hier werden nur die Benutzer angezeigt, die Mitglied der entsprechenden Gruppe sind.

3.18.2 u.trust LAN Crypt Zertifikate erzeugen und zuordnen

Dieser Assistent erzeugt Zertifikate für **alle** Benutzer, denen beispielsweise noch kein Zertifikat zugeordnet wurde und ordnet diese den Benutzern automatisch zu. Sie können mithilfe des Assistenten aber auch neue Zertifikate für solche Benutzer erzeugen, die bereits über ein Zertifikat verfügen (z. B. auch für solche Benutzer, bei denen das bisherige Zertifikat bald ablaufen würde).

Zum Öffnen dieses Assistenten klicken Sie auf **Zertifikate erzeugen** im Kontextmenü jedes Knotens *Mitglieder und Zertifikate für Gruppe* oder klicken Sie auf das entsprechende Symbol in der Symbolleiste.

Im angezeigten Dialog können Sie auswählen, ob Sie die Zertifikate nur **in dieser Gruppe** oder **in dieser Gruppe und allen Untergruppen** bzw. **nur für ausgewählte Benutzer** erzeugen und zuweisen wollen.



Wenn Sie die Option **Neue Zertifikate erstellen (auch, wenn bereits welche vorhanden sind)** markieren, werden für alle ausgewählten Benutzer neue Zertifikate erzeugt, d. h. auch dann, wenn diese Benutzer bereits ein Zertifikat haben.

Nur für ausgewählte Benutzer

Diese Option wird nur angezeigt, wenn zuvor ein oder mehrere Benutzer ausgewählt wurden. Die einzelnen Benutzer einer Gruppe werden im rechten Konsolenfenster angezeigt, wenn mit der linken Maustaste auf *Mitglieder und Zertifikate für Gruppe* unter dem entsprechenden Gruppenknoten geklickt wird. Das Markieren der Benutzer funktioniert analog zum Markieren von Dateien im Windows Explorer (Auswahl der Benutzer mit der linken Maustaste bei gedrückter Umschalt-, oder STRG-Taste bzw. durch Ziehen mit der Maus bei gedrückter linker Maustaste und gedrückter Umschalt-Taste).

Erzeugung und Zuordnung der Zertifikate erfolgen vollautomatisch. Klicken Sie auf **Fertigstellen,** um den Assistenten zu schließen.

Hinweis: Die hier erzeugten Schlüsseldateien (**.p12*) und der öffentliche Teil des Security Officer Zertifikats (**.cer*) werden in dem im Knoten **Zentrale Einstellungen** angegebenen Verzeichnis gespeichert und müssen den Benutzern zur Verfügung gestellt werden.

Dazu kann in der *u.trust LAN Crypt*-Konfiguration über eine Gruppenrichtlinie eingestellt werden, in welchem Pfad der *u.trust LAN Crypt* Client nach einer **.p12*-Datei für den Benutzer sucht, insofern der private Schlüssel zum Öffnen der Profildatei noch nicht vorhanden ist.

Gleiches gilt für den öffentlichen Teil des Security Officer Zertifikats.

Damit die Benutzer-Schlüsseldateien automatisch erkannt werden, müssen die Dateinamen dem Anmeldenamen des Benutzers entsprechen („*Anmeldename.p12*“).

Wird eine entsprechende Datei gefunden, erscheint ein PIN-Dialog. Diese PIN (enthalten in der Passwortprotokolldatei „*p12pwlog.csv*“) muss dem Benutzer, z. B. über einen PIN-Brief, mitgeteilt werden. Sowohl das Zertifikat als auch der dazugehörige Schlüssel werden nach Eingabe der PIN automatisch in den Zertifikatsspeicher importiert.

Wird eine entsprechende „**.cer*“-Datei gefunden, die den öffentlichen Teil des Security Officer Zertifikats enthält, wird auch diese automatisch importiert.

Als Alternative dazu können die Schlüsseldateien der Benutzer und der öffentliche Teil des Security Officer-Zertifikats auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide Zertifikate von den Clients importiert werden.

3.18.3 Assistent zur Zertifikatszuordnung

u.trust LAN Crypt stellt einen Assistenten zur Zertifikatszuordnung zur Verfügung, der die Zuordnung der Zertifikate zu den Benutzern weitgehend automatisiert. Den Assistenten starten Sie über die Option **Assistent zur Zertifikatszuordnung** im Kontextmenü von „*Mitglieder und Zertifikate für Gruppe*“.

Im ersten Dialog des Assistenten können Sie auswählen, ob Sie die Zertifikate nur **in diese Gruppe** oder **in dieser Gruppe und allen Untergruppen** bzw. **nur für ausgewählte Benutzer** zuordnen wollen.

Nur für ausgewählte Benutzer

Diese Option wird nur angezeigt, wenn zuvor ein oder mehrere Benutzer ausgewählt wurden. Die einzelnen Benutzer einer Gruppe werden im rechten Konsolenfenster angezeigt, wenn mit der linken Maustaste auf *Mitglieder und Zertifikate für Gruppe* unter dem entsprechenden Gruppenknoten geklickt wird. Das Markieren der Benutzer funktioniert analog zum Markieren von Dateien im Windows Explorer (Auswahl der Benutzer mit der linken Maustaste bei gedrückter Umschalt-, oder STRG-Taste bzw. durch Ziehen mit der Maus bei gedrückter linker Maustaste und gedrückter Umschalt-Taste).

Der Assistent unterstützt die Zuordnung von Zertifikaten aus folgenden Quellen:

- Zertifikate aus dem **Active Directory**
- Zertifikate aus dem **LDAP-Verzeichnis**
- Zertifikate aus einem **Dateisystemverzeichnis**
- Zertifikate aus dem **Zertifikatspeicher**

3.18.3.1 Zertifikate aus dem Active Directory zuordnen

Wenn Sie die Option Zertifikate aus dem **Active Directory** zuordnen gewählt haben, müssen Sie in Schritt 2 den Namen eines Active-Directory-Controllers in FQDN-Form angeben (z. B. „*adserver.contoso.com*“).

Durch Klicken auf **Standardwert** wird die Adresse des Domänencontrollers, an den Sie zurzeit angemeldet sind, eingetragen.

Starten Sie den Assistenten durch Klicken auf **Weiter**. Der Import und die Zuordnung der Zertifikate erfolgen vollautomatisch. Eine Meldung bestätigt die erfolgreiche Zuordnung der Zertifikate. Klicken Sie danach auf **Fertigstellen,** um den Assistenten zu schließen.

3.18.3.2 Zertifikate aus einem LDAP-Verzeichnis zuordnen

Wenn Sie die Option Zertifikate aus einem **LDAP-Verzeichnis** zuordnen gewählt haben, müssen Sie in Schritt 2 Angaben zum LDAP-Verzeichnis, aus dem die Zertifikate importiert werden sollen, machen.

Hinweis:

Microsoft AD:

Das Eingabefeld darf nicht leer bleiben. Hier ist zumindest die Angabe der beiden Bestandteile „Domäne“ und „Toplevel-Domäne“ erforderlich. „DC“ steht hierbei für „*Domain Component*“.

Beispiel 1: `DC=mydomain,DC=DE`

Beispiel 2: `OU=marketing,DC=mydomain,DC=DE`

Durch Klicken auf **Standardwert** wird die Adresse des Domänencontrollers eingetragen, an den Sie zurzeit angemeldet sind.

Zur Zuordnung der Zertifikate werden Übereinstimmungen zwischen Eigenschaften der LDAP-Benutzer und der *u.trust LAN Crypt*-Benutzer verwendet.

Folgende Eigenschaften der LDAP-Benutzer können verwendet werden:

- E-Mail-Adresse
- Allgemeiner Name (CN)
- Vollständiger Name
- NT 4.0 Kontoname
- Benutzeranmeldename (UPN)
- Nachname
- Benutzerdefiniertes Attribut

Diese Eigenschaften können als übereinstimmend mit folgenden *u.trust LAN Crypt*-Benutzereigenschaften definiert werden:

- E-Mail-Adresse
- Benutzername
- Anmeldename
- Kommentar

Wählen Sie aus, welche LDAP-Benutzereigenschaft der des *u.trust LAN Crypt*-Benutzers entsprechen soll.

Wird die Übereinstimmung festgestellt, wird das Zertifikat des LDAP-Benutzers importiert und automatisch dem entsprechenden *u.trust LAN Crypt*-Benutzer zugeordnet.

Hinweis: Zur Vermeidung von Inkonsistenzen wird die Verwendung der E-Mail-Adresse als Zuordnungskriterium empfohlen, da diese immer eindeutig sein sollte.

Starten Sie den Assistenten durch Klicken auf **Weiter**. Der Import und die Zuordnung der Zertifikate erfolgen automatisch. Eine Meldung bestätigt die erfolgreiche Zuordnung der Zertifikate. Klicken Sie danach auf **Fertigstellen,** um den Assistenten zu schließen.

3.18.3.3 Zertifikate aus einem Dateisystemverzeichnis zuordnen

Wenn Sie die Option **Zertifikate aus einem Dateisystemverzeichnis zuordnen** gewählt haben, müssen Sie in Schritt 2 des Assistenten angeben, in welchem Verzeichnis bzw. Ordner sich die Zertifikate befinden.

Nach der Angabe des Ortes können Sie im folgenden Dialog festlegen, nach welcher Methode *u.trust LAN Crypt* die Zertifikate den Benutzern zuordnen soll.

- **Benutzername entspricht Dateiname**

  Wählen Sie diese Option, wenn die Dateinamen der Zertifikatsdateien identisch mit den Benutzernamen sind.

  Allen Benutzern, denen ein Dateiname entspricht, wird das entsprechende Zertifikat zugeordnet.

- **Benutzername ist im DN enthalten**

  Ist der Benutzername im *Distinguished-Namen* des Zertifikats enthalten, so ist *u.trust LAN Crypt* in der Lage, diesen zu finden und das Zertifikat dem entsprechenden Benutzer zuzuordnen. Dazu ist ein Suchmuster erforderlich, durch das *u.trust LAN Crypt* den Benutzernamen im DN identifizieren kann.

  Das Suchmuster kann in den Eingabefeldern unter der Option **Benutzername ist im DN enthalten** festgelegt werden. Es wird nach dem Benutzernamen gesucht, der sich im DN zwischen den beiden angegebenen Zeichenfolgen befindet.

  Beispiel:

  Der Benutzername steht im DN des Zertifikats immer unter „CN=“.

  (z. B.: `CN=MaxMustermann,OU=u.trust`)

Durch Eingabe von `CN=` im ersten und `OU=u.trust` im zweiten Eingabefeld kann *u.trust LAN Crypt* den Benutzernamen, der sich zwischen den beiden Zeichenfolgen befindet, eindeutig identifizieren (im Beispiel „*MaxMustermann*“). Das Zertifikat wird dem Benutzer automatisch zugeordnet.

- **Zuordnung aus Datei entnehmen**

  Die gewünschte Zuordnung kann auch einer Datei entnommen werden.

  Zum Beispiel wird der öffentliche Teil der mit der u.trust Smartcard-Administration erzeugten Zertifikate in einer Datei in einem angegebenen Verzeichnis bzw. Ordner gespeichert. Zusammen mit diesen Dateien wird von der u.trust Smartcard-Administration eine Datei erzeugt, die die Information enthält, welchem Benutzer welches Zertifikat zugeordnet ist. Auch andere PKIs sind imstande, derartige Listen zu erzeugen. Natürlich kann diese Liste auch selbst generiert werden.

  Sie muss folgendem Format entsprechen:

  Benutzername;Dateiname

  Beispiel:

  ```
  Gast;Gastcer.cer
  MaxMustermann;Mustermann.cer
  ....
  ```

Die Zertifikate werden entsprechend der Zuordnung in dieser Datei zugeordnet.

Nach dem Klicken auf **Weiter** müssen Sie noch festlegen, wie *u.trust LAN Crypt* bestehende Zuordnungen behandeln soll.

3.18.3.4 Zertifikate aus Zertifikatsspeicher zuordnen

Wenn Sie die Option Zertifikate aus Zertifikatsspeicher zuordnen gewählt haben, werden Sie im zweiten Schritt des Assistenten gefragt, ob verfügbare Zertifikate automatisch zugeordnet, eine Liste aller verfügbaren Zertifikate erzeugt und importiert werden soll bzw. ob eine bereits vorhandene Liste importiert werden soll. Anhand dieser Liste erfolgt von *u.trust LAN Crypt* die Zuordnung der Zertifikate.

Die Option **Importieren einer vorhandenen Liste** kann z. B. verwendet werden, wenn die Zuordnung bereits einmal gestartet wurde, der Vorgang aber nach dem Erzeugen der Liste abgebrochen wurde. Die erstellte Datei kann dann wiederverwendet werden.

Wird die Option **Erzeuge und importiere eine Liste aller verfügbaren Zertifikate** gewählt, wird der folgende Dialog angezeigt.

Wählen Sie den Namen der Ausgabedatei für die Liste.

u.trust LAN Crypt erzeugt eine Liste aller im Zertifikatsspeicher verfügbaren Zertifikate. Diese Liste enthält Platzhalter für die Benutzernamen, denen das Zertifikat zugeordnet werden soll.

Beispiel:

```
*****; My; OU=U.trust LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...
*****; Root; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...
```

Die Platzhalter (*****) können durch den Benutzernamen ersetzt werden.

Ist der Benutzername im Zertifikat enthalten, kann folgende Option verwendet werden:

- **Versuche Benutzer zu erkennen**

  Ist der Benutzername im *Distinguished Name* (DN) des Zertifikats enthalten, so ist *u.trust LAN Crypt* in der Lage, diesen zu finden und das Zertifikat dem entsprechenden Benutzer zuzuordnen. Dazu ist ein Suchmuster erforderlich, durch das *u.trust LAN Crypt* den Benutzernamen im DN identifizieren kann.

  Das Suchmuster kann in den Eingabefeldern unter dieser Option festgelegt werden. Es wird nach dem Benutzernamen, der sich im DN zwischen den beiden angegebenen Zeichenfolgen befindet, gesucht.

  Beispiel:

  Der Benutzername steht im DN des Zertifikats immer unter „*CN=*“.

  (z.B. `CN=UlrikeFalke,OU=utimaco`)

  Durch Eingabe von CN= im ersten und OU=u.trust im zweiten Eingabefeld kann *u.trust LAN Crypt* den Benutzernamen, der sich zwischen den beiden Zeichenfolgen befindet, eindeutig identifizieren (im Beispiel „*UlrikeFalke*“). Der Platzhalter wird durch den Benutzernamen ersetzt und das Zertifikat wird dem Benutzer automatisch zugeordnet.

- **Ausgabedatei nach Fertigstellung mit Editor öffnen**

  Wird diese Option aktiviert, wird die Liste der Zertifikate nach dem Erzeugen geöffnet. Sie können die Liste nun bearbeiten. Die Platzhalter können bei den entsprechenden Zertifikaten durch die Benutzernamen ersetzt werden. Nach dem Abspeichern der Liste wird die editierte Version für die Zuordnung verwendet.

Nach dem Klicken auf **Weiter** müssen Sie noch festlegen, wie *u.trust LAN Crypt* bestehende Zuordnungen behandeln soll.

3.19 Bereitstellen der Verschlüsselungsregeln - Profildateien erzeugen

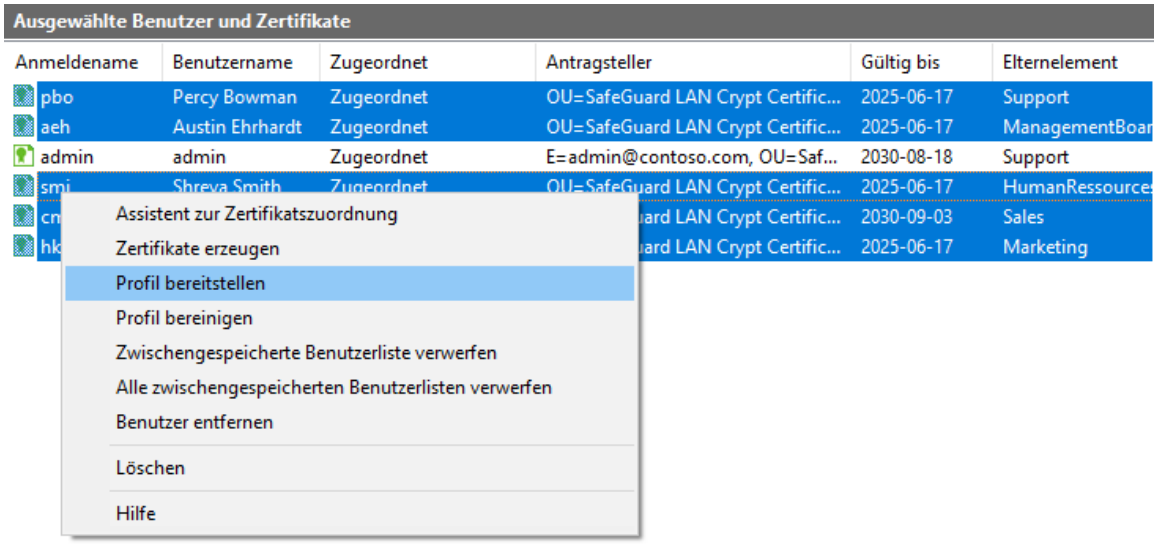
Alle Profile, die erzeugt wurden (oder insofern Änderungen in den Profilen vorgenommen wurden), werden in der *u.trust LAN Crypt*-Administrationsdatenbank gespeichert. Sie haben dann zunächst noch keine Auswirkungen auf die einzelnen Benutzer.

Um den Benutzern Zugriff auf ihre Profile zu ermöglichen, muss der Security Officer über die *u.trust LAN Crypt*-Admin-Konsole Profildateien erzeugen. Der Benutzer erhält Zugriff auf sein neues Verschlüsselungs-Profil nach dem nächsten Anmelden, oder durch Aktualisierung des Profils über das *u.trust LAN Crypt*-Clientmenü.

Hinweis: Bitte beachten Sie, dass nach Änderungen in der *u.trust LAN Crypt*-Administration (*neue Schlüssel*, *neue Regeln*, Anpassungen für *TrustBuilder MFA*, usw.) immer neue Profildateien erzeugt werden müssen. Die Änderungen für die Benutzer werden erst aktiv, wenn diese die neuen Profildateien geladen haben.

3.19.1 Erzeugen (Bereitstellen) von Profildateien für eine gesamte Gruppe oder für ausgewählte Benutzer

Profildateien werden über die *u.trust LAN Crypt* Admin-Konsole erzeugt. Mithilfe eines Assistenten können Sie zuvor ausgewählten Benutzern neue oder aktualisierte Verschlüsselungsregeln zuweisen. Der Assistent startet, wenn mehr als ein Benutzer ausgewählt wird und das Erzeugen des Profils von der Symbolleiste oder dem Kontextmenü von Benutzern aus gestartet wird.



Wird für einen einzelnen oder mehrere Benutzer aus dem Kontextmenü **Profil bereitstellen** ausgewählt, so wird das Profil unmittelbar erzeugt. Eine Meldung informiert den Security Officer über das Ergebnis.

Hinweis: Wählen Sie stattdessen **Profil bereinigen** im Kontextmenü wird für den Benutzer ein leeres Profil erstellt. Nach dem Aktualisieren des Profils über den *u.trust LAN Crypt*-Client stehen diesem Benutzer dann keine Verschlüsselungsregeln und Schlüssel mehr zur Verfügung. Ein Zugriff auf verschlüsselte Daten ist für diesen Benutzer dann nicht mehr möglich. Sie können dem Benutzer jederzeit wieder ein Profil bereitstellen. Erst bei erneuter Aktualisierung des Profils über den *u.trust LAN Crypt*-Client erhält er wieder sein Verschlüsselungsprofil mit allen für ihn definierten Regeln und Schlüsseln und er kann wieder mit verschlüsselten Daten arbeiten.

Die Ausgangspunkte für den Assistenten richten sich danach, von welcher Ansicht der Assistent gestartet wird:

- **Auswahl des Geltungsbereichs** (Standard)
- **Zusammenstellung der Benutzer und Prüfung der Zertifikate**

  Wenn keine Auswahl des Geltungsbereichs möglich ist, zum Beispiel, wenn die Profilerzeugung für ausgewählte Benutzer im Knoten **Ausgewählte Benutzer und Zertifikate** gestartet wird.

- **Erzeugen / bereinigen des Profils:**

  Wenn *Profil bereinigen* für mehrere Benutzer gestartet wird. Zertifikatsprüfungen sind an dieser Stelle nicht notwendig.

Auf der ersten Seite des Assistenten kann der Geltungsbereich für die Profilerzeugung ausgewählt werden, wenn dies für mehr als einen einzelnen Benutzer erfolgen soll. Für folgende Geltungsbereiche können Profile erzeugt werden:

- Nur Benutzer in dieser Gruppe
- Benutzer in dieser Gruppe und alle Untergruppen
- Nur ausgewählte Benutzer

  Wählen Sie die Option *Nur Richtliniendateien für geänderte Gruppen bereitstellen*, um die Erzeugung von Profildateien auf Benutzer zu beschränken, für die aufgrund von vorgenommenen Änderungen neue Profildateien erforderlich sind. Hierdurch lässt sich die Erzeugung von Profildateien in großen Organisationen beschleunigen.

Auf der zweiten Seite des Assistenten wird der Fortschritt angezeigt, während alle Benutzerdaten gesammelt und die Benutzerzertifikate geprüft werden. Wenn alle Benutzer verarbeitet sind, wird die nächste Seite angezeigt.

Auf der dritten Seite des Assistenten werden Zertifikatswarnungen angezeigt. Auf dieser Seite werden jene Benutzer angezeigt, denen bisher noch kein gültiges Zertifikat zugeordnet ist, oder deren Zertifikat bald abläuft.

Die folgenden Zertifikatswarnungen und -fehler werden angezeigt:

- Das Zertifikat des Benutzers läuft bald ab (Warnung).
- Alle zugeordneten Zertifikate des Benutzers sind abgelaufen (Fehler).
- Einem Benutzer ist kein Zertifikat zugeordnet (Fehler).
- Dem Benutzer ist kein Zertifikat zugeordnet und er ist als zu überspringen markiert (Warnung).

Wird ein Fehler angezeigt, so muss auf dieser Seite mindestens eine der folgenden Optionen ausgewählt werden, damit die Profilerzeugung fortgesetzt werden kann:

- **Für die Benutzer in der Liste nicht mehr warnen**

  Es werden alle Benutzer übersprungen, deren Zertifikate abgelaufen sind oder denen keine Zertifikate zugeordnet sind. Diese Benutzer werden in der Profilerzeugung so lange übersprungen, bis sie neue bzw. wieder gültige Zertifikate erhalten haben.

- **Benutzer ohne zugeordnetes Zertifikat immer überspringen**

  Es werden alle Benutzer ohne gültiges Zertifikat ignoriert. Dies ist eine globale Einstellung, die auch im Knoten **Zentrale Einstellungen** konfiguriert werden kann.

Klicken Sie auf **Zurück**, um zur Seite für die Auswahl des Geltungsbereichs zurückzukehren.

Die vierte Seite des Assistenten zeigt eine Fortschrittsanzeige, während alle Profile erzeugt werden. Der Assistent kann zwar abgebrochen werden, dadurch wird jedoch nur die Profilerzeugung gestoppt. Bereits erzeugte Profildateien werden nicht gelöscht oder zurückgesetzt.

Auf der fünften und letzten Seite des Assistenten wird die Anzahl an erzeugten Profilen angezeigt. Wenn ein Fehler aufgetreten ist, durch den die Profilerzeugung gestoppt werden musste, wird eine Fehlermeldung angezeigt.

Hinweis: Wenn Sie auf den Reitern **Antivirus-Software**, **Regeln auflösen** oder **Andere Einstellungen** im Knoten **Zentrale Einstellungen** Änderungen vornehmen, hat das auch Auswirkungen auf die Profildateien aller Benutzer. Nach einer Änderung dieser Art müssen neue Profildateien für alle Benutzer erzeugt werden.

3.19.2 Selektives Bereitstellen über Zertifikats-Snap-In

Das Zertifikats-Snap-In kann ebenfalls zum Bereitstellen der Profildateien verwendet werden. Es steht unter dem Knoten **Mitglieder und Zertifikate für Gruppen** und unter jedem Gruppenknoten zur Verfügung.

Das Erzeugen der Profildateien über das Zertifikats-Snap-In bietet folgende Zusatzfunktionen:

- Benutzer, denen ein Zertifikat zugewiesen werden soll, können ausgewählt werden. Es ist nicht notwendig für alle Benutzer neue Profildateien zu erzeugen.

  Mehrere Benutzer können wie im Windows-Explorer (Maus + SHIFT bzw. STRG) ausgewählt werden.

- Der Security Officer sieht sofort, welche Benutzer in der Gruppe vorhanden sind.

- Die Zertifikatssymbole neben den Benutzernamen zeigen den Status der Zertifikate an:

  - **Rotes Symbol bedeutet:**

    Das Zertifikat ist abgelaufen.

  - **Gelbes Symbol bedeutet:**

    Das Zertifikat läuft innerhalb der konfigurierten Warnfrist ab.

  - **Grünes Symbol bedeutet:**

    Alles OK.

  - **Graues Symbol bedeutet:**

    Entweder wurde dem Benutzer kein Zertifikat zugeordnet oder er wurde bei der Zuordnung der Zertifikate übersprungen.

Zum Bereitstellen der Profildateien markieren Sie die gewünschten Benutzer und klicken anschließend auf das blaue Zahnradsymbol in der Symbolleiste oder auf **Profile bereitstellen** im Kontextmenü des markierten Benutzers.

3.19.3 Profile bereinigen

Im Zertifikats-Snap-In können die Profile eines oder mehrerer Benutzer bereinigt werden. Beim Bereinigen von Profilen wird eine leere Profildatei erstellt. Der Benutzer muss sich einmal an diese Datei anmelden, damit die Einstellungen in der auf seinem Rechner zwischengespeicherten Profildatei überschrieben werden. Danach hat er auf verschlüsselte Daten keinen Zugriff mehr.

Zum Bereinigen eines Profils markieren Sie den Benutzer im Zertifikats-Snap-In und klicken auf das Symbol **Profil für gewählte Benutzer bereinigen** oder auf **Profil bereinigen** im Kontextmenü.

Sie können auch mehrere Benutzer auswählen (markieren bei gedrückter Umschalt-Taste) und deren Profil durch Klicken auf das Symbol bereinigen.

Hinweis: Über den Knoten **Zentrale Einstellungen** von *u.trust LAN Crypt* legen Sie fest, wie Profile bereinigt werden. Der Vorgang Bereinigen eines Profils ähnelt dem Vorgang Erzeugen eines Profils.

3.20 Datenbankprotokollierung

u.trust LAN Crypt protokolliert ausgewählte Ereignisse in der *u.trust LAN Crypt*-Datenbank. Die Protokollierung bietet die Möglichkeit, bestimmte Ereignisse festzuhalten, diese Information zu archivieren und jederzeit überprüfen zu können.

Über die globalen Rechte **Protokoll lesen** und **Protokollierung verwalten** lassen sich die Zugriffsrechte der Security Officer auf die Protokollierung von *u.trust LAN Crypt* einstellen. Diese hierzu erforderlichen Rechte kann der Master Security Officer für jeden Security Officer entsprechend einstellen.

Protokoll lesen	Für den Security Officer sind die Einstellungen für die Protokollierung und die Einträge in das Protokoll sichtbar.
Protokollierung verwalten	Der Security Officer darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.

Die Grundeinstellungen zur Protokollierung werden in der *u.trust LAN Crypt*-Admin-Konsole über den Knoten **Protokollierung** unter dem Knoten **Zentrale Einstellungen** vorgenommen. Dieser Knoten ist für einen Security Officer nur dann sichtbar, wenn dieser zumindest das Recht **Protokoll lesen** besitzt.

Die Basiseinstellungen können nur von einem Master Security Officer vorgenommen werden. Sie können darüber hinaus durch eine zusätzliche Autorisierung abgesichert werden (**Protokollierung verwalten** erfordert bei einem Security Officer die globalen Rechte **Protokoll lesen** und **Protokoll verwalten**).

Zu den Grundeinstellungen zählt auch die Auswahl von Ereignissen, die protokolliert werden sollen. Diese Auswahl kann ebenfalls nur von einem Master Security Officer vorgenommen werden.

Hinweis: Ereignisse, die vor der Anmeldung eines Security Officers eintreten, können nicht unmittelbar in der Datenbank protokolliert werden. Sie werden zwischengespeichert und bei der nächsten erfolgreichen Anmeldung in die Datenbank übertragen.

3.20.1 Einstellungen

Durch Klicken auf *Eigenschaften* im Knoten **Protokollierung** wird der Dialog zum Festlegen der Grundeinstellungen geöffnet.

Register Einstellungen

Im Register **Einstellungen** des Knotens **Protokollierung** wird das Mindestalter von Protokolleinträgen, bevor sie gelöscht werden können, angegeben.

Mit dieser Einstellung soll sichergestellt werden, dass beim Einsatz von verteilten Datenbanken die Einträge sicher zur Zentrale repliziert werden, bevor sie in den einzelnen Niederlassungen gelöscht werden können.

Register Status

Im Register **Status** werden Informationen über den Stand der Protokollierung angezeigt. Es werden dort Informationen angezeigt, wie viele Einträge protokolliert wurden. Sind mehrere Standorte vorhanden, erweitert sich die Anzeige pro Standort. Darüber hinaus wird dort angezeigt, wie viele Einträge bereits archiviert sind und ob diese auch gelöscht werden können.

3.20.2 Protokollierte Ereignisse

Nach Öffnen des Knotens **Protokollierung** per Mausklick, werden im rechten Konsolenfenster die Ereignisse angezeigt, die für eine Protokollierung zur Verfügung stehen. Hier können Sie auswählen, welche Aktionen protokolliert werden.

Hinweis: Die Auswahl, welche Aktionen protokolliert werden sollen, kann nur von einem Master Security Officer vorgenommen werden.

Durch Klicken auf die Spaltenüberschrift **Stufe** können Sie die Ereignisse nach Kategorien sortieren (Notfall, Alarm, Kritisch, Fehler, Warnung, Notiz, Information).

Einträge werden durch einen Doppelklick oder durch Klicken auf das entsprechende Symbol in der Symbolleiste zur Protokollierung ausgewählt.

- Aktiviert die Protokollierung für ausgewählte Ereignisse.
- Deaktiviert die Protokollierung für ausgewählte Ereignisse.

Durch Klicken bei gedrückter Umschalt- oder STRG-Taste können Sie auch mehrere Aktionen gleichzeitig auswählen.

Nachdem die Einträge ausgewählt wurden, müssen Sie die Einstellungen durch Klicken auf das Disketten-Symbol speichern. Dies können Sie alternativ auch über das Menü *Aktion* und nach Auswahl von *Änderungen speichern*. Außerdem werden Sie beim Verlassen dieser Ansicht gefragt, ob die geänderten Einträge gespeichert werden sollen.

3.20.3 Einträge ansehen und exportieren

Hinweis: Zum Ansehen und Exportieren der protokollierten Einträge benötigt ein Security Officer das Recht **Protokoll lesen**.

Ein Security Officer, der das globale Recht **Protokoll lesen** besitzt, kann sich die protokollierten Einträge anzeigen lassen und diese Einträge in eine Datei exportieren.

Die Einträge werden durch Klicken auf **Einträge ansehen und exportieren** im Kontextmenü des Knotens **Protokollierung** bzw. durch Klicken auf das Symbol in der Symbolleiste angezeigt.

 Öffnet den Dialog zum Ansehen und Exportieren der protokollierten Ereignisse.

Im angezeigten Dialog werden alle Ereignisse, die für die Protokollierung aktiviert wurden, angezeigt.

Durch Klicken auf die jeweiligen Spaltenüberschriften können die Einträge sortiert werden.

Ein Doppelklick auf einen Eintrag zeigt Details zum protokollierten Ereignis an.

Zusätzlich stellt *u.trust LAN Crypt* einen Filter zur Verfügung, über den Bedingungen für die angezeigten Ereignisse angegeben werden können.

3.20.4 Filtern

Die Einstellungen für die Protokollierung können im Knoten **Protokollierung** definiert werden. Für die Anzeige und für den Export der protokollierten Ereignisse steht eine Filterfunktion zur Verfügung. Diese kann, wenn der Knoten **Protokollierung** markiert ist, über das Kontextmenü (rechte Maustaste) bzw. das Menü **Aktion** über **Einträge ansehen und exportieren** entsprechend definiert werden.

Durch Klicken auf **Filtern** im Dialog der protokollierten Ereignisse wird ein Dialog angezeigt, in dem ein Filter für die protokollierten Ereignisse definiert werden kann.

Für das Filtern der Ereignisse können folgende Parameter angegeben werden:

- **Nur Einträge eines bestimmten Ereignisses anzeigen**

  Wird diese Option ausgewählt, werden nur die Einträge für die in der Drop-Down-Liste ausgewählte Aktion angezeigt. Die Liste enthält alle protokollierbaren Ereignisse.

- **Nur Einträge eines bestimmten Security Officer anzeigen**

  Wird diese Option ausgewählt, kann in der Drop-Down-Liste ein Security Officer ausgewählt werden. Es werden dann nur die Ereignisse angezeigt, die protokolliert wurden, als dieser Security Officer an der *u.trust LAN Crypt* Admin-Konsole angemeldet war. Die Drop-Down-Liste enthält nur solche Security Officer, für die auch Protokolleinträge vorhanden sind.

- **Nur Ereignisse einer bestimmten Stufe anzeigen**

  Wird diese Option ausgewählt, kann mit den beiden Drop-Down-Listen eine einzelne Kategorie bzw. ein Bereich von Kategorien angeben werden, der angezeigt werden soll. *Stufe ist höchstens* und *Stufe ist mindestens* beziehen sich auf die Zahl vor der jeweiligen Kategorie.

- **Nur Ereignisse einer bestimmten Zeitspanne anzeigen**

  Wird diese Option ausgewählt, kann eine Zeitspanne angegeben werden, in der die angezeigten Einträge liegen sollen.

- **Nur Ereignisse mit einem bestimmten Status anzeigen**

  Wird diese Option aktiviert, kann ausgewählt werden, ob nur noch nicht archivierte oder nur archivierte Beiträge (bereits archivierte Einträge verbleiben in der Datenbank, bis sie gelöscht werden) angezeigt werden sollen. Wird die Option nicht aktiviert, werden immer alle Einträge angezeigt.

- **Nur Ereignisse eines bestimmten Standortes anzeigen**

  Wird diese Option aktiviert, werden nur die Ereignisse, die an einem bestimmten Standort protokolliert wurden, angezeigt. Verschiedene Standorte existieren nur, wenn mit einer verteilten Datenbank gearbeitet wird. Welche Standorte sichtbar sind, hängt davon ab, wie die Datenbank repliziert wird.

Hinweis: Auch nach dem Ausführen der Funktion **Einträge ansehen und exportieren** kann der Filter durch Klicken auf die Schaltfläche **Filter** im Ergebnis-Dialog "*Ereignisse ansehen*" definiert werden. Alternativ steht diese Funktion auch über das Menü **Ansicht** und nach Auswahl von **Filter** zur Verfügung.

3.20.5 Einträge archivieren, löschen, prüfen

Hinweis: Zum Archivieren, Löschen und Prüfen der protokollierten Einträge benötigt ein Security Officer das globale Recht **Protokollierung verwalten**. Erhält der Security Officer dieses Recht, wird automatisch auch das globale Recht **Protokoll lesen** gewährt.

Ein Security Officer, der das globale Recht **Protokollierung verwalten** besitzt, kann protokollierte Einträge archivieren, löschen und prüfen.

Durch Klicken auf **Einträge archivieren, löschen und prüfen** im *Kontextmenü* des Knotens **Protokollierung** bzw. durch Klicken auf das Symbol in der Symbolleiste wird für diese Aktionen ein Assistent gestartet.

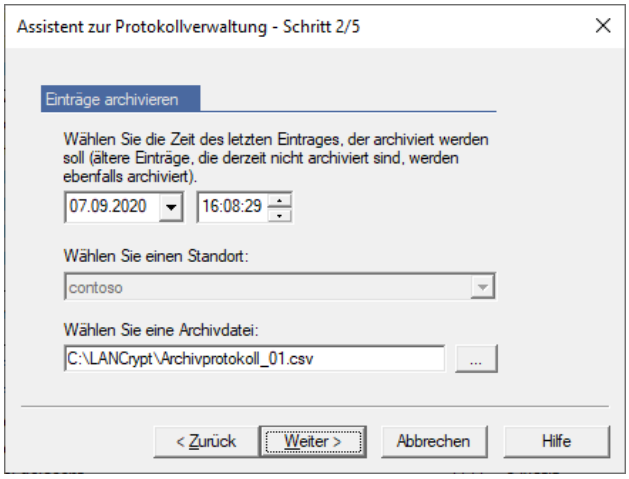
 Startet einen Assistenten zum Archivieren, Löschen und Prüfen protokollierter Ereignisse.

Einträge archivieren

Zum Archivieren von Einträgen markieren Sie **Einträge archivieren** und klicken Sie auf **Weiter**.

Im nächsten Dialog können Sie festlegen:

- Datum und Zeit des letzten Eintrags, der archiviert werden soll. Alle früheren Einträge vor diesem Zeitpunkt, die bisher nicht archiviert sind, werden ebenfalls archiviert. Zudem können Sie an dieser Stelle die Archivierung auch nach Standorten (soweit vorhanden) vornehmen.



Hinweis: Verschiedene Standorte existieren nur, wenn mit einer verteilten Datenbank gearbeitet wird. Welche Standorte an dieser Stelle wählbar sind, hängt davon ab, wie die Datenbank repliziert wird. In der Grafik oben besteht z. B. nur ein Standort. Als Standort gilt immer der Eintrag, den Sie während der Installation von *u.trust LAN Crypt* definiert haben. Dieser lässt sich nachträglich nicht ändern.

- Den Namen der Datei, in der die Einträge archiviert werden sollen.

Klicken Sie auf **Weiter**. Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden. Klicken Sie auf **Weiter**. Sind alle Einträge archiviert, wird die letzte Seite des Assistenten angezeigt. Klicken Sie dort auf **Fertig stellen,** um den Assistenten zu schließen.

Archivierte Einträge verbleiben in der Datenbank und können gelöscht werden. Sie werden auf den Status *Archiviert* gesetzt.

Archivierte Einträge löschen

Um archivierte Einträge zu löschen, klicken Sie auf **Einträge löschen** und danach auf **Weiter**.

Hinweis: Wenn noch keine Einträge archiviert wurden, können Einträge nicht gelöscht werden.

Im nächsten Dialog können Sie festlegen:

- Datum und Uhrzeit des letzten Eintrags, ab welchem Zeitpunkt gelöscht werden soll. Alle früheren Protokolleinträge vor diesem Zeitpunkt (auch wenn diese noch nicht archiviert sind) werden gelöscht.

  Hinweis: Der letzte mögliche Zeitpunkt ist abhängig vom angegebenen Mindestalter von Protokolleinträgen, welches Sie im Register **Einstellungen** über den Knoten **Protokollierung** definieren können.

- Standort, dessen Einträge (soweit vorhanden) gelöscht werden sollen.

Klicken Sie auf **Weiter**.

Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden.

Klicken Sie auf **Weiter**. Sind die Einträge gelöscht, wird die letzte Seite des Assistenten angezeigt. Klicken Sie auf die Schaltfläche **Fertig stellen,** um den Assistenten zu schließen.

Archiveinträge prüfen

Zum Prüfen der Integrität der Protokollereignisse klicken Sie auf **Einträge prüfen** und danach auf **Weiter**.

Im nächsten Dialog können Sie festlegen, welche Daten geprüft werden sollen. Es können die Daten einer Datenbank oder eines Archivs geprüft werden.

Soll eine Datenbank geprüft werden, können Sie bei verteilten Datenbanken den Standort der zu prüfenden Datenbank auswählen.

Soll ein Archiv geprüft werden, können Sie die gewünschte Archivdatei über die Schaltfläche **Durchsuchen** auswählen.

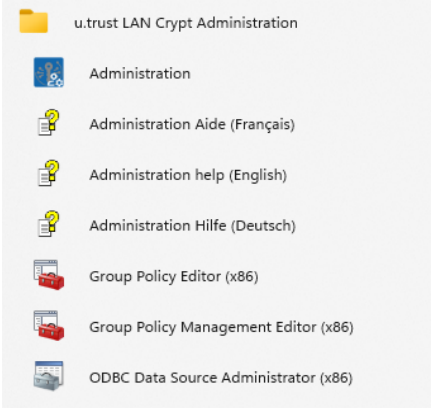
Klicken Sie auf **Weiter**. Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden.

Klicken Sie auf **Weiter**. Sind alle Einträge geprüft, wird die letzte Seite des Assistenten angezeigt. Dieser Dialog zeigt das Ergebnis der Prüfung an. Wurden die geprüften Daten manipuliert, wird eine entsprechende Meldung angezeigt.

Klicken Sie auf die Schaltfläche **Fertig stellen,** um den Assistenten zu schließen.

4 u.trust LAN Crypt Konfiguration

Hinweis: Konfigurationseinstellungen müssen mit der 32-Bit-Gruppenrichtlinien-Verwaltungskonsole (*GPME.msc*) oder dem 32-Bit-Editor für lokale Gruppenrichtlinien (*GPEdit.msc*) definiert werden. Beide Editoren sind verlinkt im Startmenü unter **u.trust LAN Crypt Administration**. Sie stellen damit sicher, dass die richtige Version gestartet wird.



Hinweis: Wenn Sie die Konfiguration der *u.trust LAN Crypt* Gruppenrichtlinien für einen Domänencontroller auf einem Windows 11-Rechner mithilfe eines Snap-Ins als Administrator durchführen wollen, müssen Sie die administrativen Vorlagendateien von *u.trust LAN Crypt* installieren (siehe u. a. Hinweis auf dieser Seite). Auf einem unterstützten Windows Server System können Sie hierzu als Administrator alternativ auch die 32-Bit-Gruppenrichtlinien-Verwaltungskonsole (*GPME.msc*) verwenden.

Die folgenden Einstellungen sind computer- oder benutzerspezifische Einstellungen. Um diese Einstellungen zu bearbeiten, benötigen Sie Administratorrechte in der Domäne oder im Active Directory. Sie sollten nur vom Systemadministrator vorgenommen werden.

Die Konfigurationseinstellungen werden über den Knoten **u.trust LAN Crypt Konfiguration** vorgenommen. Dieser Knoten wird bei der Arbeit mit Systemrichtlinien in der Management Konsole unter jedem Computerknoten und unter jedem Benutzerknoten angezeigt. In einer Active Directory-Umgebung wird der Knoten **u.trust LAN Crypt Konfiguration** in jeder Gruppenrichtlinie unter *Computerkonfiguration / Richtlinien / Windows-Einstellungen* bzw. *Benutzerkonfiguration / Richtlinien / Windows Einstellungen / u.trust LAN Crypt* angezeigt.

Hinweis: Alternativ können Sie die administrativen Vorlagendateien (**.admx* bzw. **.adml*) aus dem Ordner \Config Ihres extrahierten Installationspakets verwenden. Die ADMX-Dateien sind in den Ordner "`Windows\PolicyDefinitions`" zu kopieren oder - wenn vorhanden - in den Central Store. Die jeweiligen Sprachdateien (*.ADML) sind dagegen in den entsprechenden Länderkürzel-Ordner (z. B. "`de-DE`" für deutschsprachige *.ADML-Dateien) zu kopieren. Sie werden direkt beim nächsten Öffnen des Gruppenrichtlinien-Editors gelesen und auf ihre Syntax geprüft. Weitere Informationen über administrative Vorlagendateien finden Sie unter: `https://learn.microsoft.com/de-de/troubleshoot/windows-client/group-policy/create-and-manage-central-store`

Im Normalfall werden die Konfigurationseinstellungen computerspezifisch vorgenommen. Die Möglichkeit, diese auch benutzerspezifisch vorzunehmen, ermöglicht es bestimmten Benutzern spezielle Einstellungen zukommen zu lassen. Wenn Sie **benutzerspezifische** Einstellungen vorgenommen haben, so **überschreiben** diese die maschinenspezifischen Einstellungen.

Sollen einmal getroffene benutzerspezifische Einstellungen wieder aufgehoben werden, damit wieder die Computereinstellungen ausgewertet werden, muss die entsprechende Einstellung auf **Nicht konfiguriert** gesetzt werden. Markieren Sie dazu die betreffende Einstellung und drücken Sie die **Entfernen**-Taste. In der Management-Konsole wird in der Spalte *Konfiguriert* dann **Nein** angezeigt.

4.1 Client-Einstellungen

Bei markiertem Knoten **Client-Einstellungen** werden im rechten Konsolenfenster die konfigurierbaren Einstellungen angezeigt. Ein Doppelklick auf einen Eintrag öffnet jeweils einen Dialog, in dem die Einstellungen vorgenommen werden können.

4.1.1 Ver-/Entschlüsselung erlauben

Die Benutzeranwendung von *u.trust LAN Crypt* erlaubt die Ver- und Entschlüsselung von Dateien durch einen Eintrag im Kontextmenü des Dateiexplorers. Mit einem Rechtsklick auf eine Datei stehen dann im Kontextmenü unter dem Eintrag *u.trust LAN Crypt* erweiterte Funktionen zur Verfügung. Auf diese Weise können auch Dateien verschlüsselt werden, für die keine Regel definiert wurde.

Soll das verhindert werden, kann hier festgelegt werden, dass diese Möglichkeit im Kontextmenü von Dateien nicht angeboten wird.

Ver-/Entschlüsselung erlauben: nein

Verhindert, dass Dateien, für die keine Verschlüsselungsregel definiert wurde, über das Kontextmenü ver-/entschlüsselt werden.

4.1.2 Fehler bei der Zertifikatsüberprüfung ignorieren

u.trust LAN Crypt erlaubt festzulegen, ob mögliche Fehler bei der Überprüfung der Zertifikate der Benutzer ignoriert werden.

Ein Anlass für eine solche Vorgehensweise kann sein, dass die Gültigkeitsdauer der Zertifikate abläuft und noch keine neuen Zertifikate zur Verfügung stehen. Um sicherzustellen, dass die Benutzer weiterhin Zugriff auf ihre Verschlüsselungsprofile haben, kann bis zur Verteilung der neuen Zertifikate die Prüfung der Gültigkeitsdauer ignoriert werden. Damit können diese an sich abgelaufenen Zertifikate noch weiterverwendet werden. Sind die neuen Zertifikate verfügbar, kann die Einstellung **Gültigkeitsdauer ignorieren** wieder aufgehoben werden.

Hinweis: Fehler bei der Zertifikatsprüfung zu ignorieren, bedeutet immer auch eine Senkung des Sicherheitsniveaus.

- **Widerruf des Zertifikats ignorieren**

  Wenn sich das Zertifikat auf einer **C**ertificate **R**evocation **L**ist befindet, die bei der Anmeldung ausgewertet wird, darf es eigentlich nicht zur Anmeldung verwendet werden. Wird diese Option aktiviert, kann der Benutzer das Zertifikat trotzdem verwenden, um Zugriff auf sein Verschlüsselungsprofil zu haben.

- **Gültigkeitsdauer ignorieren**

  Obwohl die Gültigkeitsdauer abgelaufen ist, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil verwendet werden.

- **Ungültigen Zertifizierungspfad ignorieren**

  Obwohl der öffentliche Teil des Zertifikats des Ausstellers auf dem Client nicht vorhanden ist oder sich nicht im richtigen Zertifikatsspeicher befindet, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil verwendet werden, wenn diese Option aktiviert ist.

- **Unbekannten Widerruf ignorieren**

  Die PKIs mancher Hersteller tragen nicht standardisierte Gründe für den Widerruf eines Zertifikats in eine CRL ein. In der Regel ist ein Zertifikat nicht erlaubt, auch wenn der Grund des Widerrufs nicht bekannt ist. Wird diese Option aktiviert, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil dennoch weiterhin verwendet werden.

Hinweis: Bitte beachten Sie, dass das Ignorieren von Fehlern bei der Zertifikatsprüfung in den meisten Fällen auch ein Umgehen der Sicherheitsrichtlinien eines Unternehmens bedeutet. Der *u.trust LAN Crypt Client* erkennt, übereinstimmend mit RFC 5280, einen unbekannten Grund nicht an. Geben Sie deshalb zum Widerruf eines Zertifikats einen anderen Grund an.

Diese Einstellungen können auch unter den Server-Einstellungen definiert werden. Zertifikate werden sowohl bei der Anmeldung eines Security Officers an der *u.trust LAN Crypt* Admin-Konsole als auch bei der Durchführung einer zusätzlichen Autorisierung geprüft.

4.1.3 Alle Umgebungsvariablen verwenden

Die Umgebungsvariable %USERNAME% in Pfadangaben wird von *u.trust LAN Crypt* standardmäßig aufgelöst (ausgenommen sind Pfade in *Bypass-Regeln*).

Hier können Sie festlegen, ob auch andere Umgebungsvariablen in Pfadangaben aufgelöst werden sollen.

Der Einsatz anderer Umgebungsvariablen in Pfadangaben kann problematisch werden, wenn die Benutzer in der Lage sind, diese zu ändern. Dies kann dazu führen, dass Pfadangaben im Verschlüsselungsprofil ihre Wirkung verlieren.

4.1.4 Menüeinträge aktivieren

Hier können Sie festlegen, welche Menüeinträge im *u.trust LAN Crypt*-Benutzermenü auf den Client-Rechnern sichtbar sind. In der Standardeinstellung werden alle Menüeinträge angezeigt. Deaktivieren Sie hier einen Menüeintrag, wird er auf dem Client-Rechner nicht angezeigt. Damit

steht diese Funktionalität auf diesem Client nicht zur Verfügung. So können Sie zum Beispiel verhindern, dass die Verschlüsselung auf einem Client-Rechner deaktiviert wird.

4.1.5 Standard 'Ignorieren Regel'

Da beim Booten eines Client-Computers der *u.trust LAN Crypt*-Treiber geladen wird, werden bereits alle Dateien auf eine mögliche Verschlüsselung und damit auf die entsprechenden Zugriffsrechte geprüft, auch wenn noch kein benutzerspezifisches Verschlüsselungsprofil geladen ist. Dies kann zu Performance-Einbußen in dieser Phase führen.

Mithilfe einer computerspezifischen Einstellung in der *u.trust LAN Crypt*-Konfiguration kann der *u.trust LAN Crypt*-Treiber angewiesen werden, bestimmte Ordner, Pfade oder Laufwerke zu ignorieren und damit die Zugriffsrechte erst dann zu prüfen, wenn das Verschlüsselungsprofil des Benutzers geladen ist.

Doppelklicken Sie auf den Eintrag **Standard** '**Ignorieren Regel**' in den Client-Einstellungen, um einen Dialog zu öffnen, in dem bestimmte Laufwerke oder Ordner (z. B. "c:*.*;c:\windows*.*") angegeben werden können, die vom *u.trust LAN Crypt*-Treiber ignoriert werden sollen.

Werden mehrere Pfade angegeben, sind diese durch ein Semikolon voneinander zu trennen.

Bei der Verwendung von solchen Regeln muss aber berücksichtigt werden, dass dann auch die *u.trust LAN Crypt* spezifische Zugriffskontrolle auf verschlüsselte Dateien entfällt, und zwar so lange, bis das Verschlüsselungsprofil des Benutzers geladen ist.

Beispiel:

Wenn Sie "c:*.*;d:*.*" als **Standard 'Ignorieren Regel'** angeben, so wird der Treiber angewiesen, alle Ordner und Unterordner auf den Laufwerken „C" und „D" zu ignorieren, bis das Verschlüsselungsprofil des Benutzers geladen wird.

Auch beim Einsatz von *u.trust LAN Crypt* auf einem Terminal-Server kann die **Standard 'Ignorieren Regel'** zu einem Performance-Gewinn führen. Arbeiten auf dem Terminal-Server z. B. mehrere Benutzer, von denen nur einer *u.trust LAN Crypt* verwendet, kann der Treiber so angewiesen werden, die Sessions der anderen Benutzer zu ignorieren. Da diese kein Verschlüsselungsprofil geladen haben, gilt für sie nur die **Standard 'Ignorieren Regel'**.

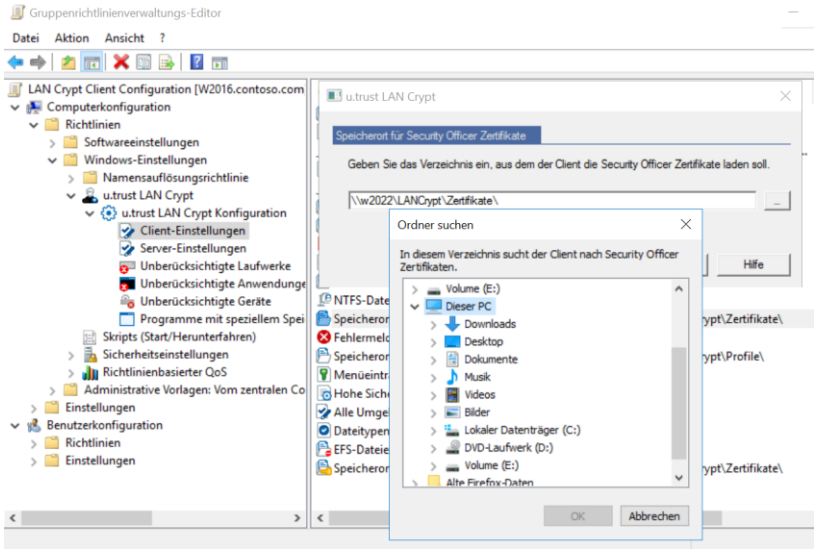
Hinweis: Bitte beachten Sie, dass die Einträge, die Sie an dieser Stelle definieren, dann auch immer alle vorhandenen Unterordner miteinschließen.

Hinweis: Bitte beachten Sie, dass bei einer Neuinstallation (kein Update) von *u.trust LAN Crypt* die **Standard 'Ignorieren Regel'** mit dem Wert "*" vordefiniert ist. Dies hat zur Folge, dass der spezifische Zugriffsschutz von *u.trust LAN Crypt* so lange für alle Pfade und Dateien inaktiv ist, bis das Profil des Benutzers geladen wurde. Benutzer könnten ggf. in dieser Zeitspanne oder auch, wenn diese ihr Profil entladen haben, verschlüsselte Dateien löschen. Das gilt auch dann, wenn sie für die dort gespeicherten Dateien keinen Schlüssel besitzen.

Sie können dies ändern, indem Sie einen oder mehrere Pfade für die **Standard 'Ignorieren Regel'** definieren (z. B. "`c:\meine_verschlüsselten_dateien\*.*`").

4.1.6 Speicherort für Security Officer Zertifikate

Zur Angabe des Speicherorts markieren Sie *Client-Einstellungen* und klicken Sie im rechten Konsolenfenster auf **Speicherort für Security Officer Zertifikate** doppelt.



Nach Angabe eines Pfads bzw. Auswahl des Ordners versucht *u.trust LAN Crypt,* automatisch das Security Officer-Zertifikat aus diesem Pfad zu importieren, falls das Zertifikat für die betreffende Profildatei des Benutzers nicht vorhanden ist. Als Ergebnis werden von der Client-Anwendung alle(!) **.cer*-Dateien aus dem angegebenen Pfad importiert.

4.1.7 Speicherort für Schlüsseldatei

Zur Angabe des Speicherorts markieren Sie *Client-Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Speicherort für Schlüsseldatei**.

Nach Angabe eines Pfads versucht die *u.trust LAN Crypt-Clientanwendung*, automatisch eine *.p12-Schlüsseldatei für den Benutzer zu importieren, falls der private Schlüssel zum Öffnen der Profildatei nicht vorhanden ist. Diese Datei muss "*Anmeldename.p12*" heißen, damit sie für den betreffenden Benutzer erkannt wird.

Beide oben beschriebenen Pfade sind standardmäßig nicht gesetzt, d. h. es erfolgt kein automatisches Laden des öffentlichen Teils des Security Officer-Zertifikats bzw. der Zertifikate bzw. Schlüsseldateien der Benutzer. Ein automatisches Laden erfolgt erst, nachdem der Systemadministrator diese Pfade explizit gesetzt hat.

Die *u.trust LAN Crypt*-Administration speichert sowohl die Schlüsseldateien (**.p12*-Dateien) für die Benutzer als auch den öffentlichen Teil des Security Officer Zertifikates (**.cer*) in denselben Ordner. Aus Client-Sicht sind die Pfade trotzdem getrennt konfigurierbar, um eventuell eine der beiden Funktionen abschalten zu können. Im Normalfall werden diese beiden Pfade daher aber gleich sein. Sollen öffentliche Security Officer-Zertifikate und Benutzerschlüsseldateien automatisch aus verschiedenen Pfaden geladen werden, müssen sie manuell in die entsprechenden Pfade bzw. Ordner kopiert werden.

4.1.8 Speicherort für Richtliniendatei

Zur Angabe des Speicherorts markieren Sie *Client-Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Speicherort für Richtliniendatei**.

Geben Sie den Pfad für den Speicherort der benutzerspezifischen Richtlinien- bzw. Profildatei ein. Um sicherzustellen, dass Clients auf ihre Profildateien zugreifen können (zum Beispiel auf einer Netzwerkfreigabe), muss der Pfad aus der Sicht des Clients angegeben werden.

Üblicherweise ist dies der gleiche Ordner, in dem der Security Officer die Profildateien für die Benutzer über die *u.trust LAN Crypt*-Admin-Konsole erzeugt. Es muss unbedingt die UNC-Schreibweise (Universal Naming Convention) verwendet werden, da zu diesem Zeitpunkt noch keine Laufwerke verbunden sind!

Die Umgebungsvariable %LOGONSERVER% kann bei dieser Einstellung verwendet werden (dies gilt für Load Balancing oder ähnliches).

Die in der Gruppenrichtlinie eingetragenen Pfade für Security Officer-Zertifikate, Schlüsseldateien und Richtlinien- bzw. Profildateien müssen mit den definierten Pfaden in der Admin-Konsole im Knoten **Zentrale Einstellungen**, Reiter **Verzeichnisse** übereinstimmen.

4.1.9 Zwischenspeicherort für Richtliniendatei

Zur Angabe des Zwischenspeicherorts markieren Sie *Client-Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Zwischenspeicherort für Richtliniendatei**.

In diesem Ordner wird eine lokale Kopie der Richtlinien- bzw. Profildatei gespeichert. Die Profildatei wird normalerweise von einem Netzwerkverzeichnis gelesen. Der Benutzer muss über Schreibrechte in dem entsprechend angegebenen lokalen Ordner verfügen. Damit kann sichergestellt werden, dass ein Verschlüsselungsprofil eines Benutzers weiterhin verfügbar ist, auch wenn einmal keine Netzwerkverbindung besteht.

Es kann entweder einer der vorgeschlagenen Speicherorte (Windows Standard-Ordner) aus der Liste verwendet werden, oder es wird nach der Auswahl von <*Andere*> ein beliebiger Pfad im Eingabefeld eingetragen.

Hinweis: Bei den angebotenen Speicherorten handelt es sich um Windows Standard-Ordner, die vom verwendeten Betriebssystem abhängig sind. <*Lokale Anwendungsdaten*> bezieht sich immer auf einen Ordner auf der lokalen Maschine, während sich alle anderen unter Umständen (z. B. Roaming Users) auch auf Netzwerklaufwerken befinden können.

Wird ein Speicherort manuell angegeben, muss sichergestellt werden, dass der Ordner auf den Client-Rechnern auch existiert.

Hinweis: Wenn Sie einen Benutzer aus Ihrer *u.trust LAN Crypt*-Umgebung entfernen wollen, müssen Sie bedenken, dass die lokale Kopie auf dem Rechner gespeichert bleibt. Solange dies der Fall ist, kann der Benutzer mit den darin enthaltenen Rechten auf Daten zugreifen. Um dies zu vermeiden, sollten Sie für diesen Benutzer eine leere Profildatei erzeugen. Löschen Sie hierzu dessen Profildatei und entfernen Sie diesen Benutzer aus allen Gruppen (siehe „*Profile bereinigen*“ auf Seite 169).

4.1.10 Verzögerung beim Laden des Profils

Hier können Sie eine Zeitspanne in Sekunden angeben, die gewartet wird, bis das Profil des Benutzers geladen wird. Diese Verzögerung ist z. B. dann von Bedeutung, wenn ein Zertifikat auf einem Token verwendet wird. Die Verzögerung beim Laden des Profils stellt sicher, dass auf den Token oder die Smartcard zugegriffen werden kann, wenn das Zertifikat benötigt wird. Typischer Wert: 20 Sekunden.

4.1.11 Dateitypen für den Assistenten zur Initialverschlüsselung

Wenn Sie hier bestimmte Dateitypen angeben, werden ausschließlich Dateien vom angegebenen Typ vom Assistenten zur Initialverschlüsselung bearbeitet. Der Benutzer kann diese Einstellung im Assistenten zur Initialverschlüsselung nicht verändern!

Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert.

Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Ordner, für den eine Verschlüsselungsregel besteht, bleiben diese bei der Initialverschlüsselung unberücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden.

Möchten Sie den Benutzer die Möglichkeit geben, diese Einstellung im Assistenten zur Initialverschlüsselung selbst vorzunehmen, belassen Sie diese Einstellung auf **Nicht konfiguriert**.

Haben Sie hier Dateitypen angegeben und wollen zu einem späteren Zeitpunkt dem Benutzer die Auswahl vornehmen lassen, müssen Sie diese Einstellung wieder auf **Nicht konfiguriert** setzen.

Hinweis: Diese Einstellung gilt nur für den Assistenten zur Initialverschlüsselung. Wird die Verschlüsselung über die Explorer-Erweiterung „*Gemäß Profil verschlüsseln*“ gestartet, hat dies keine Auswirkung.

Verwenden Sie zur Angabe der Dateitypen eine durch Semikola getrennte Liste.

Beispiel: `docx;xlsx;pdf;txt`

4.1.12 Dauer der Zwischenspeicherung der Richtliniendatei

Standardverhalten von u.trust LAN Crypt

Wenn sich ein Benutzer an Windows anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach überprüft *u.trust LAN Crypt*, ob es eine neue Profildatei für den Benutzer gibt, indem es eine Verbindung zum festgelegten Speicherort für Profildateien (Netzwerklaufwerk) aufbaut. Wird dort eine neuere Profildatei gefunden, wird das zwischengespeicherte Benutzerprofil aktualisiert.

Diese Vorgehensweise hat den Vorteil, dass der Benutzer bereits mit verschlüsselten Daten arbeiten kann, während *u.trust LAN Crypt* überprüft, ob es eine neuere Version der Profildatei gibt.

Ist das Netzwerklaufwerk nicht erreichbar, arbeitet der Benutzer so lange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

Ist diese Option auf **Nicht konfiguriert** gesetzt, verhält sich *u.trust LAN Crypt* wie oben beschrieben.

Mit dieser Einstellung können Sie das Standardverhalten verändern.

Hinweis: Sie können eine Einstellung auf **Nicht konfiguriert** setzen, indem Sie diese markieren, und in ihrem Kontextmenü (Klick mit der rechten Maustaste) auf **Löschen** klicken. In der Spalte *Konfiguriert* wird neben der relevanten Option jetzt **Nein** angezeigt.

Sie können hier angeben, wie lange die zwischengespeicherte Richtlinie auf den Client-Computern gültig ist.

Innerhalb des angegebenen Zeitraums ist die Profildatei auf dem Client gültig und der Benutzer hat Zugriff auf verschlüsselte Daten, auch wenn keine Verbindung zum Speicherort der Profildatei im Netzwerk besteht.

Der Zeitraum, wie lange die Profildateien zwischengespeichert werden und damit gültig bleiben, kann in Tagen oder Wochen angegeben werden.

Läuft die angegebene Zeit ab, versucht *u.trust LAN Crypt* noch einmal, die Profildatei vom Netzwerklaufwerk zu laden, um sie zu aktualisieren. Ist dies nicht möglich, wird die Profildatei entladen. Der Benutzer hat keinen Zugriff mehr auf verschlüsselte Daten. Erst wenn wieder eine gültige Profildatei zur Verfügung steht (z. B. bei der nächsten Anmeldung mit einer Verbindung zum Speicherort der Profildatei für die Clients), wird die Profildatei aktualisiert und geladen. Der Benutzer hat wieder Zugriff auf verschlüsselte Daten. Der Zähler für die Dauer der Zwischenspeicherung wird zurückgesetzt.

Die Angabe der Dauer der Zwischenspeicherung kann sicherstellen, dass die Client-Computer in regelmäßigen Intervallen mit aktuellen Profildateien versorgt werden und die Benutzer in der Folge immer aktuelle Verschlüsselungsregeln verwenden. Denn solange die Profildateien durch eine Verbindung zum Speicherort für Profildateien nicht aktualisiert werden, kann ein Benutzer mit einer zwischengespeicherten Version der Profildatei unbegrenzt lange arbeiten, wenn diese Einstellung auf **Nicht konfiguriert** gesetzt ist.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung zurückgesetzt:

- Der Speicherort der Profildateien ist erreichbar, es wurde eine gültige Profildatei auf den Client übertragen (z. B. bei der Anmeldung des Benutzers, oder ausgelöst durch ein eingestelltes Aktualisierungsintervall), diese ist aber nicht neuer als die bestehende.
- Eine neue Profildatei ist verfügbar und wurde erfolgreich geladen.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung **NICHT** zurückgesetzt:

- Der Client-Computer versucht, eine neue Profildatei zu erhalten. Der Speicherort der Profildatei ist jedoch nicht erreichbar.
- Eine neue Profildatei wurde übertragen. Sie konnte aber aufgrund eines Fehlers nicht geladen werden.
- Es ist eine neue Profildatei verfügbar. Diese Profildatei verlangt aber ein neues Zertifikat (z. B., wenn die Profildatei von einem anderen Security Officer erstellt wurde). Der Benutzer besitzt dieses Zertifikat nicht oder kann es nicht laden.

Schlägt die Aktualisierung der Profildatei fehl, wird auf dem Client-Computer der Ablaufzeitpunkt der zwischengespeicherten Profildatei in Form einer Sprechblasen-Hilfe angezeigt. Der Benutzer kann dann eine manuelle Aktualisierung über das *u.trust LAN Crypt*-Tray-Icon anstoßen. Eine automatische Aktualisierung wird auch entsprechend analog zu den Einstellungen unter *Aktualisierungsintervall für das Benutzerprofil* durchgeführt.

Keine Zwischenspeicherung der Richtliniendatei

Wenn Sie die Dauer der Zwischenspeicherung auf „0“ setzen, wird die Profildatei nicht zwischengespeichert. Das bedeutet, dass der Benutzer sein Benutzerprofil bei der Anmeldung erhält, sobald der Speicherort der Profildatei erreichbar ist. Ist dieser nicht erreichbar oder tritt ein Fehler beim Laden des Profils auf, kann der Benutzer nicht auf verschlüsselte Daten zugreifen.

4.1.13 NTFS-Datei-Dekomprimierung

Diese Einstellung ermöglicht die Bearbeitung von NTFS komprimierten Dateien durch den Assistenten zur Initialverschlüsselung. Wird die Option **NTFS-Dateidekomprimierung** auf **Ja** gesetzt, dekomprimiert der Assistent NTFS-komprimierte Dateien und verschlüsselt sie anschließend, wenn für sie eine Verschlüsselungsregel gilt.

Ist die Option **NTFS-Dateidekomprimierung** auf **Nein** gesetzt, werden NTFS-komprimierte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht verschlüsselt, auch wenn für sie eine Verschlüsselungsregel festgelegt wurde.

Wird diese Option konfiguriert, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung nicht ändern! Nur wenn diese Option auf **Nicht konfiguriert** gesetzt wird, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung selbst vornehmen.

4.1.14 EFS-Dateientschlüsselung

Diese Einstellung ermöglicht die Bearbeitung von EFS-verschlüsselten Dateien durch den Assistenten zur Initialverschlüsselung. Wird die Option **EFS-Dateientschlüsselung** auf **Ja** gesetzt, entschlüsselt der Assistent EFS-verschlüsselte Dateien und verschlüsselt sie anschließend, wenn für sie eine *u.trust LAN Crypt*-Verschlüsselungsregel gilt.

Ist die Option **EFS Dateientschlüsselung** auf **Nein** gesetzt, werden EFS-verschlüsselte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht von *u.trust LAN Crypt* umgeschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

Wird diese Option konfiguriert, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung nicht ändern! Nur wenn diese Option auf **Nicht konfiguriert** gesetzt wird, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung selbst vornehmen.

Hinweis: Sie können eine Einstellung auf **Nicht konfiguriert** setzen, indem sie diese markieren, und in ihrem Kontextmenü (Klick mit der rechten Maustaste) auf **Löschen** klicken. In der Spalte *Konfiguriert* wird neben der relevanten Option jetzt **Nein** angezeigt.

4.1.15 Aktualisierungsintervall für das Benutzerprofil

Diese Einstellung legt fest, wie oft *u.trust LAN Crypt* überprüft, ob eine neue Profildatei zur Verfügung steht und diese bei Bedarf aktualisiert.

Um eine Aktualisierung durchführen zu können, muss *u.trust LAN Crypt* Zugriff auf das Netzwerklaufwerk haben, auf dem sich die Profildateien befinden. Es wird geprüft, ob dort eine neuere Version der Profildatei existiert. In dem Fall wird die Profildatei dann auf dem Client-Computer aktualisiert. *u.trust LAN Crypt* führt alle für das erfolgreiche Laden des Benutzerprofils notwendigen Schritte (wenn notwendig neue Zertifikate suchen und verifizieren, etc.) automatisch durch. Nur wenn kein Fehler dabei aufgetreten ist, wird das alte durch das neue Benutzerprofil ersetzt und geladen. Danach wird der Zähler für die Dauer der Zwischenspeicherung zurückgesetzt. Sind beide Profildateien identisch, wird der Zähler ebenfalls zurückgesetzt.

Das Aktualisierungsintervall kann in Minuten, Stunden, Tagen und Wochen angegeben werden.

Hinweis: *u.trust LAN Crypt* lässt keine Aktualisierungsintervalle zu, die kürzer als 15 Minuten sind. Ist diese Option auf **Nicht konfiguriert** gesetzt, werden Profildateien nicht automatisch aktualisiert.

4.1.16 Fehlermeldung nicht anzeigen - wenn kein Benutzerprofil gefunden

u.trust LAN Crypt zeigt in der Standardeinstellung eine Fehlermeldung an, wenn kein Benutzerprofil gefunden wird.

Hier können Sie festlegen, dass diese Fehlermeldung unterdrückt wird, wenn kein Benutzerprofil gefunden wird.

Wird die Option **Fehlermeldung nicht anzeigen** auf **Ja** gesetzt, wird die Anzeige der Fehlermeldung unterdrückt.

Hinweis: Diese Einstellung kann insbesondere in Terminal-Server-Umgebungen hilfreich sein, wenn nicht alle Benutzer mit *u.trust LAN Crypt* arbeiten sollen.

4.1.17 Persistente Verschlüsselung

Dateien bleiben normalerweise nur so lange verschlüsselt, wie sie einer Verschlüsselungsregel unterliegen. Wenn zum Beispiel ein Benutzer eine verschlüsselte Datei aus einem Pfad, für den eine Verschlüsselungsregel besteht, in einen Ordner kopiert, für den keine Verschlüsselungsregel gilt, wird die Datei im Zielordner entschlüsselt. Durch Aktivierung der persistenten Verschlüsselung kann der Security Officer dafür sorgen, dass Dateien auch dann weiterhin verschlüsselt bleiben, wenn sie an einen Speicherort verschoben oder kopiert werden, für den keine Verschlüsselungsregel gilt.

Die Funktion deaktivieren Sie durch einen Doppelklick auf **Persistente Verschlüsselung** und Auswahl von **nein** aus dem Listenfeld hinter **Persist. Verschlüsselung aktivieren**.

Standardmäßig ist diese Funktion für den Client aktiviert.

4.1.18 Hohe Sicherheit für den privaten Schlüssel

Hier können Sie festlegen, dass der Benutzer jedes Mal zur Authentisierung aufgefordert wird, wenn der private Schlüssel von *u.trust LAN Crypt* verwendet wird. Wenn Sie diese Einstellung aktivieren, gilt diese auch für den Security Officer (siehe „*Hohe Sicherheit für den privaten Schlüssel*“ im Abschnitt „*Server-Einstellungen*“ auf Seite 187).

Hinweis: Bitte beachten Sie, dass diese Richtlinie keinen Einfluss auf bereits importierte oder manuell installierte Zertifikate hat. Wenn Sie diese Einstellung aktivieren, gilt diese nur für Zertifikate, die danach über *u.trust LAN Crypt* importiert werden.

4.1.19 Zufallszahlengenerator

Zur sicheren Schlüsselgenerierung setzt *u.trust LAN Crypt* einen integrierten Zufallszahlengenerator ein. Hier können Sie einstellen, welchen Algorithmus der Zufallszahlengenerator verwenden soll. Die Auswahl wirkt sich dabei auf die Sicherheit der erzeugten Schlüssel aus. *BasicRandom* bietet eine gute Performance bei moderater Sicherheit und eignet sich für Systeme mit begrenzten Ressourcen und wird von allen früheren *LAN Crypt* Versionen unterstützt. *AdvancedRandom* bietet eine ausgewogene Balance zwischen guter Entropie und Performance. *SuperRandom* hingegen liefert eine deutlich höhere Entropie und wird für Umgebungen empfohlen, für die besonders hohe Sicherheitsanforderungen gelten.

Hinweis: *SuperRandom* wird erst ab *u.trust LAN Crypt* Version 13.0.0 unterstützt.

Wählen Sie aus dem Listenfeld einen Algorithmus für den Zufallszahlengenerator aus:

- BasicRandom
- AdvancedRandom
- SuperRandom

Falls Sie die Einstellung für den Zufallszahlengenerator auf **Nicht konfiguriert** setzen, verwendet *u.trust LAN Crypt* standardmäßig *SuperRandom*.

Hinweis: Den Algorithmus für den Zufallszahlengenerator können Sie sowohl in den *Client*- als auch in den *Server-Einstellungen* einstellen (siehe „*Zufallszahlengenerator*“ im Abschnitt „*Server-Einstellungen*“ auf Seite 188). Für beide Einstellungen kann jedoch immer nur derselbe Algorithmus gelten. Ändern Sie den Algorithmus für den Zufallsgenerator in einer der beiden Einstellungen, erfolgt analog hierzu die Änderung auch bei der anderen Einstellung.

4.1.20 Erstellen von Klartextdateien nicht zulassen

Mit dieser Einstellung können Sie verhindern, dass Klartextdateien in definierten Netzwerkpfaden, auf verbundenen Netzlaufwerken oder lokalen Laufwerken erstellt werden, wenn noch kein *u.trust LAN Crypt* Benutzerprofil geladen ist oder der Benutzer über kein Profil verfügt. Sie können an dieser Stelle sowohl Netzwerkpfade als auch Laufwerksbuchstaben eintragen.

Beispiel:

```
\\server1\share1\
\\server2\share2\
X:
Y:
Z:
```

4.2 Server-Einstellungen

Hinweis: Diese Einstellungen müssen unbedingt für den Server gesetzt sein. Sie haben für die Client-Rechner (Ausnahme: „*Hohe Sicherheit für den privaten Schlüssel*“) keine Auswirkung.

Wenn Sie die Standardeinstellungen **nicht** verwenden, müssen Sie die *Server-Einstellungen* unbedingt konfigurieren, bevor die Administration zum ersten Mal gestartet wird!

4.2.1 Hohe Sicherheit für den privaten Schlüssel

Hier können Sie festlegen, dass der (Master) Security Officer jedes Mal, wenn der private Schlüssel von *u.trust LAN Crypt* verwendet wird, zur Authentisierung aufgefordert wird. Wenn Sie diese Einstellung aktivieren, gilt diese automatisch auch für die Clients (siehe „*Hohe Sicherheit für den privaten Schlüssel*“ im Abschnitt „*Client-Einstellungen*“ auf Seite 186).

Hinweis: Ergänzende Informationen hierzu finden Sie im Abschnitt 2.1.1 „*Sicherheitsniveau*“ auf Seite 19.

Hinweis: Auf Computer, auf denen Sie das *u.trust LAN Crypt* ScriptingAPI einsetzen, müssen Sie über die Gruppenrichtlinie diese Einstellung deaktivieren. Durch die Passwortabfrage wäre andernfalls beim Ausführen eines Skriptes immer eine Benutzerinteraktion erforderlich.

4.2.2 SQL-Dialekt

Hier muss der SQL-Dialekt, der für die Kommunikation mit der ODBC-Datenquelle verwendet wird, angegeben werden.

Wählen Sie aus:

- MS SQL-Server
- Oracle
- Standard-SQL

Die gewählte Einstellung wird dann in Ihrer Systemkonfiguration verwendet.

4.2.3 Datenbankbesitzer

Damit die verwendete Datenbank korrekt angesprochen werden kann, muss hier der Datenbankbesitzer angegeben werden.

Für den MS SQL-Server darf der Standardwert „dbo“ des Datenbankbesitzers nicht verändert werden. Eine Änderung ist nur bei Verwendung einer Oracle-Datenbank erforderlich.

Achtung: Bei Verwendung einer Oracle Datenbank müssen Sie den Datenbankbesitzer unbedingt in **GROSSBUCHSTABEN** angeben. Es muss sich hier um denselben Namen handeln, der während der Erzeugung der Datenbanktabellen verwendet wurde.

4.2.4 ODBC-Datenquelle

Hier kann der Name, mit dem auf die ODBC-Datenquelle verwiesen werden soll, konfiguriert werden.

Standardmäßig verwendet *u.trust LAN Crypt* **SGLCSQLServer** als Namen für die ODBC-Datenquelle. Wollen Sie einen anderen Namen verwenden, müssen Sie ihn hier angeben, bevor die *u.trust LAN Crypt*-Administration das erste Mal gestartet wird.

Hinweis: Der Name der hier angegebenen ODBC-Quelle unterscheidet nach Groß- und Kleinschreibung! Er muss hier genauso angegeben werden wie bei der Erstellung der ODBC-Quelle. **Es können nur 32 Bit ODBC-Datenquellen verwendet werden.**

4.2.5 Zufallszahlengenerator

Zur sicheren Schlüsselgenerierung setzt *u.trust LAN Crypt* einen integrierten Zufallszahlengenerator ein. Hier können Sie einstellen, welchen Algorithmus der Zufallszahlengenerator verwenden soll. Die Auswahl wirkt sich dabei auf die Sicherheit der erzeugten Schlüssel aus. *BasicRandom* bietet eine gute Performance bei moderater Sicherheit und eignet sich für Systeme mit begrenzten Ressourcen und wird von allen früheren *LAN Crypt* Versionen unterstützt. *AdvancedRandom* bietet eine ausgewogene Balance zwischen guter Entropie und Performance. *SuperRandom* hingegen liefert eine deutlich höhere Entropie und wird für Umgebungen empfohlen, für die besonders hohe Sicherheitsanforderungen gelten.

Hinweis: *SuperRandom* wird erst ab *u.trust LAN Crypt* Version 13.0.0 unterstützt.

Wählen Sie für den Zufallszahlengenerator einen der folgenden Algorithmen aus:

- BasicRandom
- AdvancedRandom
- SuperRandom

Falls Sie die Einstellung für den Zufallszahlengenerator auf **Nicht konfiguriert** setzen, verwendet *u.trust LAN Crypt* standardmäßig *SuperRandom*.

Hinweis: Den Algorithmus für den Zufallszahlengenerator können Sie sowohl in den *Server-* als auch in den *Client-Einstellungen* einstellen (siehe „*Zufallszahlengenerator*“ im Abschnitt „*Client-Einstellungen*“ auf Seite 186). Für beide Einstellungen kann jedoch immer nur derselbe Algorithmus gelten. Ändern Sie den Algorithmus für den Zufallsgenerator in einer der beiden Einstellungen, erfolgt analog hierzu die Änderung auch bei der anderen Einstellung.

4.2.6 Fehler bei Zertifikatsüberprüfung ignorieren

Hier können Sie angeben, welcher Zertifikatsstatus ignoriert werden soll, wenn sich ein Security Officer anmeldet oder wenn über die Admin-Konsole Zertifikate zugewiesen werden.

4.2.7 Hash-Algorithmus

Der verwendete Hash-Algorithmus wird an dieser Stelle nur angezeigt.

4.2.8 Zertifikatserweiterung prüfen

Standardmäßig werden von *u.trust LAN Crypt* bei der Zuweisung aus dem Zertifikatsspeicher nur Zertifikate angeboten, die als Eigenschaft unter Schlüsselverwendung *Schlüsselverschlüsselung* und / oder *Datenverschlüsselung* eingetragen haben.

Unter **Zertifikatserweiterung prüfen** kann jedoch eingestellt werden, dass diese Prüfung entfällt und so auch Zertifikate mit anderen Eigenschaften zur Verwendung mit *u.trust LAN Crypt* zugelassen werden.

Zertifikatserweiterungen prüfen: **Nein** ermöglicht die Verwendung von Zertifikaten mit anderen Eigenschaften.

Hinweis: Werden solche Zertifikate eingesetzt, ist es jedoch vom verwendeten CSP oder KSP abhängig, ob diese Zertifikate auch mit *u.trust LAN Crypt* genutzt werden können.

Sollten Sie diese Prüfung ausschalten, stellen Sie bitte sicher, dass die verwendeten Zertifikate mit *u.trust LAN Crypt* genutzt werden können.

4.2.9 Performance beim Erstellen von Profilen optimieren

Mit dieser Einstellung können Sie die Performance beim Erstellen von Profildateien verändern. Standardmäßig wird beim Erstellen einer Profildatei die temporäre Profildatei in das Resolver-

Cache-Verzeichnis `%LOCALAPPDATA%\Utimaco\ResolverCache` geschrieben, von dort kopiert und anschließend gelöscht.

Bei der Einstellung **Ja** wird die temporäre Profildatei dagegen bei der Profilerstellung sofort in das Ausgabeverzeichnis verschoben. Dies führt zu einer verbesserten Leistung bei der Erzeugung von Profildateien.

Hinweis: Wenn Sie die Einstellung **Performance beim Erstellen von Profilen optimieren** aktivieren und sich das Resolver-Cache-Verzeichnis und das Ausgabeverzeichnis auf dem gleichen Speichermedium befinden, erhalten die im Ausgabeverzeichnis erzeugten Profildateien jedoch die vom Resolver-Cache-Verzeichnis geerbte ACL, anstelle der vom Ausgabeverzeichnis geerbten ACL.

Falls Sie diese Einstellung auf **Nicht konfiguriert** oder **nein** setzen, wird beim Erstellen einer Profildatei die temporäre Profildatei weiterhin standardmäßig in das Resolver-Cache-Verzeichnis geschrieben, von dort kopiert und anschließend gelöscht.

4.3 Unberücksichtigte Laufwerke, Anwendungen und Geräte

u.trust LAN Crypt erlaubt die Definition von Laufwerken, Anwendungen und Geräten (Netzwerk-Dateisysteme), die vom *u.trust LAN Crypt* Filter-Treiber ignoriert werden sollen und damit von der transparenten Ver-/Entschlüsselung ausgenommen sind.

Ein Beispiel für eine unberücksichtigte Anwendung kann ein Backup-Programm sein. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung / Entschlüsselung ausgenommen werden. Die Daten bleiben bei jeder Sicherung dann weiterhin verschlüsselt.

Das Ausschließen ganzer Laufwerke führt zu einem Performance-Gewinn. Soll beispielsweise auf dem Laufwerk „E“ keine Verschlüsselung stattfinden, wird es einfach als „Unberücksichtigtes Laufwerk“ markiert. Alternativ könnte man eine Regel für dieses Laufwerk mit der Option „Ignorierenregel für diesen Pfad“ definieren.

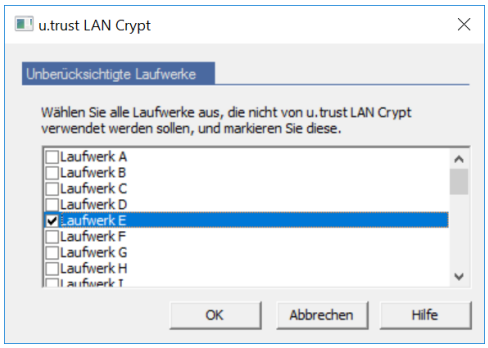
Durch die Definition als „Unberücksichtigtes Laufwerk“ entfällt aber die Abarbeitung des Profils durch den Filter-Treiber, sodass in der Folge Dateioperationen schneller durchgeführt werden können.

Sie finden diese Einstellungen unter dem Knoten **LAN Crypt Konfiguration**.

Hinweis: Da es sich dabei um computerspezifische Einstellungen handelt, werden diese erst nach einem Neustart der Client-Rechner wirksam.

4.3.1 Unberücksichtigte Laufwerke hinzufügen

Markieren Sie *Unberücksichtigte Laufwerke* und klicken Sie im Kontextmenü auf **Unberücksichtigte(s) Laufwerk(e)** hinzufügen.



Markieren Sie die Laufwerke, die *u.trust LAN Crypt* nicht berücksichtigen soll, und klicken Sie auf **OK**.

4.3.2 Unberücksichtigte Anwendungen hinzufügen

Markieren Sie *Unberücksichtigte Anwendungen* und klicken Sie im Kontextmenü auf **Unberücksichtigte Anwendungen hinzufügen**.

Typische Verwendung:

- Backup-Programme können als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern können.
- Auch Komprimierungsprogramme können als unberücksichtigt definiert werden, wenn verschlüsselte Dateien mit solchen Programmen nicht unverschlüsselt in ein Archiv hinzugefügt werden sollen.
- Anwendungen, die bei gleichzeitiger Verwendung mit *u.trust LAN Crypt* Funktionsstörungen auslösen können, aber keine Verschlüsselung benötigen, können generell von der Verschlüsselung ausgenommen werden.

Um eine unberücksichtigte Anwendung anzugeben, müssen Sie den vollständigen Namen der ausführbaren Datei dieser Anwendung eingeben.

Geben Sie den Namen und den Pfad (falls erforderlich) der Anwendung ein.

Sollen auch die untergeordneten Prozesse (Kindprozesse) dieser Anwendungen durch den *u.trust LAN Crypt* Filter-Treiber ignoriert werden, markieren Sie die Option **Einschließlich untergeordneter Kindprozesse** und klicken Sie auf **OK**.

Hinweis: *u.trust LAN Crypt* behandelt standardmäßig bestimmte Anwendungen bereits als „*Unberücksichtigte Anwendungen*“. Bevor Sie eine Anwendung als „*Unberücksichtigte Anwendung*“ angeben, prüfen Sie über die *u.trust LAN Crypt* Client Benutzeranwendung zunächst über den **Client-Status** (dort im Reiter „*Ausnahmen*“, Abschnitt „*Unberücksichtigte Anwendungen*“), ob diese Anwendung ggf. dort bereits standardmäßig definiert ist.

4.3.3 Unberücksichtigte Geräte hinzufügen

Markieren Sie *Unberücksichtigte Geräte* und klicken Sie im Kontextmenü auf **Unberücksichtigte Geräte hinzufügen**.

Im Dialog *Unberücksichtigte Geräte* können Sie Netzwerk-Dateisysteme und bestimmte Laufwerkstypen auswählen, die von *u.trust LAN Crypt* nicht berücksichtigt werden sollen. Daten, die sich auf Speicherorten befinden, die Sie als *Unberücksichtigte Geräte* definiert haben, werden von *u.trust LAN Crypt* nicht verschlüsselt. Aus technischen Gründen ist es nicht möglich, hier einzelne Netzwerklaufwerke auszuschließen.

Hinweis: Einzelne (Netzwerk-)Laufwerke können vom Security Officer durch das Anlegen einer entsprechenden Verschlüsselungsregel von der Verschlüsselung ausgenommen werden.

Neben den bekannten Netzwerk-Dateisystemen können auch Geräte durch die Angabe ihres Gerätenamens ausgeschlossen werden. Dies kann nützlich sein, wenn Dateisysteme von Drittanbietern verwendet werden, die von einer Verschlüsselung ausgenommen werden sollen.

Folgende vordefinierte Geräte können gewählt werden:

- Client für Microsoft Netzwerke
- Microsoft Client für Netware
- Novell-Client für Netware
- Citrix-Client Laufwerkszuordnung
- Multiple UNC Provider

sowie folgende zusätzliche Geräte nach Typ:

- 1 (=Startvolumen)
- 2 (=Wechselmedien)
- 4 (=Optische Laufwerke)
- 8 (=Lokale Festplatten)
- 15 (=Alle lokalen Laufwerke)
- 16 (=Netzwerkfreigaben)

Administratoren können Werkzeuge wie z. B. OSRs *DeviceTree* verwenden, um sich die Namen der auf dem System verwendeten Dateisysteme anzeigen zu lassen.

5 Anhang

5.1 Rechteprotokollierung

.... Rechte für 'Security Officer_Utimaco-NI' wurden hinzugefügt. Zulassen: 0x86000000 - Verweigern: 0x0)...

Aus den Werten hinter **Zulassen:** und **Verweigern:** ist ersichtlich, welche Rechte konkret bearbeitet wurden.

Die folgenden Tabellen dienen zur Interpretation der Werte:

Zulassen: 0x86000000

ACL für Security Officer: Lesen	0x80000000
ACL für Security Officer: Zertifikat ändern	0x02000000
ACL für Security Officer: Region ändern	0x04000000
Zulassen:	0x86000000

Globale Rechte des Security Officers

Rechte	Werte
Security Officer erzeugen	0x000001
Profile erzeugen	0x000002
Schlüssel erzeugen	0x000004
Schlüssel kopieren	0x000008
Schlüssel entfernen	0x000010
Schlüssel lesen	0x000020
Zertifikate erzeugen	0x000040
Zertifikate zuweisen	0x000080
Gruppen ändern	0x000200
Anmeldung an Datenbank	0x000400
Operationen autorisieren	0x000800
Benutzer ändern	0x001000
Regeln erzeugen	0x002000

Rechte	Werte
Globale Rechte ändern	0x004000
ACL ändern	0x008000
Spezifische Schlüssel verwenden	0x010000
Konfiguration ändern	0x020000
Protokoll lesen	0x040000
Protokollierung verwalten	0x080000
Verzeichnisobjekte importieren	0x100000

ACL für eine Gruppe

Schlüssel erzeugen	0x00000001
Schlüssel kopieren	0x00000002
Schlüssel entfernen	0x00000004
Regeln erzeugen	0x00000008
Zertifikate zuweisen	0x00000010
Benutzer hinzufügen	0x00000020
Benutzer löschen	0x00000040
Gruppe hinzufügen	0x00000080
Untergruppe entfernen	0x00000100
Gruppen verschieben	0x00000200
Eigenschaften ändern	0x00000400
Gruppe löschen	0x00000800
Profile erzeugen	0x00001000
ACL ändern	0x00002000
Lesen	0x00004000
Sichtbar	0x00008000

ACL für Security Officer

Rechte	Werte
Namen ändern	0x01000000
Zertifikat ändern	0x02000000
Region ändern	0x04000000
Konfiguration zuordnen	0x08000000
SO löschen	0x10000000
Globale Rechte ändern	0x20000000
ACL ändern	0x40000000
Lesen	0x80000000

5.2 Rechte

5.2.1 Globale Rechte

Rechte	Beschreibung
Security Officer anlegen	Der Security Officer hat das Recht, weitere Security Officer zu erzeugen.
Profile erzeugen	Der Security Officer hat die globale Berechtigung, den Profile-Resolver zu starten und Profildateien für einzelne Benutzer zu erzeugen. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung **Profile erzeugen** für eine spezifische Gruppe für einen Security Officer gesetzt werden kann. **Profile erzeugen** berechtigt den Security Officer zum Erstellen von Profilen für Benutzer, wenn der Security Officer die Berechtigung **Profile erzeugen** für die übergeordnete Gruppe des Benutzers hat. Diese Berechtigung ist eine Voraussetzung für das Zuweisen von Werten zu Schlüsseln. Ein Security Officer, der nur die Berechtigung **Schlüssel erzeugen** hat, kann nur Schlüssel ohne Werte erzeugen.
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung **Profile erzeugen** gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung **Profile für alle Mitglieder erzeugen** für eine spezifische Gruppe gesetzt werden kann. **Profile für alle Mitglieder erzeugen** berechtigt einen Security Officer zum Erzeugen von Profilen für alle Benutzer, wenn der Security Officer die Berechtigung **Profile erzeugen** für die übergeordnete Gruppe des Benutzers oder die Berechtigung **Profile für alle Mitglieder erzeugen** für eine der Gruppen hat, zu denen der Benutzer gehört. **Hinweis:** Da die globale Berechtigung **Profile erzeugen** eine Voraussetzung für **Profile für alle Mitglieder erzeugen** ist, gilt: Wenn Sie die Berechtigung **Profile erzeugen** deaktivieren, wird auch die Berechtigung **Profile für alle Mitglieder erzeugen** deaktiviert. Wenn Sie die Berechtigung **Profile für alle Mitglieder erzeugen** aktivieren, wird automatisch auch die Berechtigung **Profile erzeugen** aktiviert.

Rechte	Beschreibung
Schlüssel erzeugen	Der Security Officer darf Schlüssel in den einzelnen Gruppen erzeugen. Das Recht **Schlüssel erzeugen** selbst erlaubt dem Security Officer nur das Erzeugen von *Schlüsseln ohne Wert*! In der Administration können *Schlüssel ohne Wert* Benutzern / Gruppen zugeordnet werden. Der Wert selbst wird erst generiert, wenn der Profile-Resolver gestartet wird. Um direkt beim manuellen Anlegen auch den zum Schlüssel gehörenden Wert erzeugen zu können, benötigt der Security Officer das Recht **Profile erzeugen**.
Schlüssel kopieren	Der Security Officer darf Schlüssel kopieren.
Schlüssel entfernen	Der Security Officer darf Schlüssel aus den Gruppen entfernen.
Schlüssel lesen	Der Security Officer darf die Daten zu den einzelnen Schlüsseln der Gruppe sehen.
Zertifikate erzeugen	Der Security Officer darf Zertifikate für die Benutzer erzeugen.
Zertifikate zuweisen	Der Security Officer darf den Benutzern Zertifikate zuweisen. Der Security Officer darf den Assistenten zur Zertifikatszuweisung starten. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung **Zertifikate zuweisen** für eine spezifische Gruppe für einen Security Officer gesetzt werden kann. **Zertifikate zuweisen** berechtigt den Security Officer zum Zuweisen von Zertifikaten zu Benutzern, wenn der Security Officer die Berechtigung **Zertifikate zuweisen** für die übergeordnete Gruppe des Benutzers hat.

Rechte	Beschreibung
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung **Zertifikate zuweisen** gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung **Zertifikate allen Mitgliedern zuweisen** für eine spezifische Gruppe gesetzt werden kann. **Zertifikate allen Mitgliedern zuweisen** berechtigt einen Security Officer zum Zuweisen von Zertifikaten zu Benutzern, wenn der Security Officer die Berechtigung **Zertifikate zuweisen** für die übergeordnete Gruppe des Benutzers oder die Berechtigung **Zertifikate allen Mitgliedern zuweisen** für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung **Zertifikate zuweisen** eine Voraussetzung für **Zertifikate allen Mitgliedern zuweisen** ist, gilt: Wenn Sie die Berechtigung **Zertifikate zuweisen** deaktivieren, wird auch die Berechtigung **Zertifikate allen Mitgliedern zuweisen** deaktiviert. Wenn Sie die Berechtigung **Zertifikate allen Mitgliedern zuweisen** aktivieren, wird automatisch auch die Berechtigung **Zertifikate zuweisen** aktiviert.
Gruppen verwalten	Der Security Officer darf Änderungen in den Gruppen vornehmen: Untergruppen aufnehmen, Gruppen verschieben, Gruppen synchronisieren, Gruppen löschen.
Anmeldung an DB	Der Security Officer darf sich an der *u.trust LAN Crypt*-Datenbank anmelden. Dieses Recht ist standardmäßig immer aktiviert. Dieses Recht stellt eine Möglichkeit dar, einem Security Officer ohne großen Aufwand die Möglichkeit zu nehmen, an der Datenbank Veränderungen vorzunehmen (z. B., wenn er das Unternehmen verlässt). Personen, die ausschließlich *Vier-Augen-Aktionen* autorisieren dürfen, kann dieses Recht verweigert werden. Damit ist sichergestellt, dass sie neben der Autorisierung von *Vier-Augen-Aktionen*, keine Möglichkeit haben, selbst Änderungen in *u.trust LAN Crypt* vorzunehmen.
Operationen autorisieren	Der Security Officer darf an *Vier-Augen-Aktionen* teilnehmen.
Benutzer verwalten	Der Security Officer darf Benutzer in eine Gruppe aufnehmen / entfernen und Gruppen synchronisieren.

Rechte	Beschreibung
Benutzer kopieren	Der Security Officer darf Benutzer zu Gruppen hinzufügen (kopieren). Diese globale Berechtigung ist eine Voraussetzung für das Setzen der Berechtigung **Benutzer kopieren** für eine spezifische Gruppe für einen Security Officer. Um einen Benutzer zu einer Gruppe hinzuzufügen, muss der Benutzer die Berechtigung **Benutzer kopieren** für die übergeordnete Gruppe des Benutzers haben.
Regeln erzeugen	Der Security Officer darf Verschlüsselungsregeln erzeugen.
Globale Rechte ändern	Der Security Officer darf die globalen Rechte eines anderen Security Officers ändern.
ACL ändern	Der Security Officer darf die ACL einer Gruppe ändern.
Spezifische Schlüssel verwenden	Der Security Officer darf bestimmte konkrete Schlüssel in Verschlüsselungsregeln verwenden und sich bestimmte Schlüssel im Knoten **Alle u.trust LAN Crypt Schlüssel** anzeigen lassen.
Konfiguration ändern	Der Security Officer darf die Konfiguration (die Pfade) ändern. Dieses Recht ist die Voraussetzung dafür, dass der Reiter **Konfigurationen** im Knoten **Zentrale Einstellungen** angezeigt wird und der Reiter **Verzeichnisse** bearbeitbar ist, wenn dieser Security Officer an die Datenbank angemeldet ist.
Protokoll lesen	Für den Security Officer sind die Einstellungen für die Protokollierung und die Protokolleinträge sichtbar.
Protokollierung verwalten	Der Security Officer darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.
Verzeichnisobjekte importieren	Der Security Officer darf OUs, Gruppen und Benutzer aus einem Verzeichnisdienst importieren und in die *u.trust LAN Crypt*-Datenbank übertragen. Dieses Recht bedingt, dass der Security Officer die Rechte **Gruppen verwalten** und **Benutzer verwalten** besitzt. Sie werden automatisch gesetzt, wenn das Recht **Verzeichnisobjekte importieren** ausgewählt wird. Besitzt ein Security Officer dieses Recht nicht, ist der Knoten **Verzeichnis-Objekte**, der das Importieren von OUs, Gruppen und Benutzern ermöglicht, in der Admin-Konsole nicht sichtbar.

5.2.2 Rechte zum Bearbeiten der Einstellungen für einen Security Officer

Rechte	Beschreibung
Namen ändern	Der hinzugefügte Security Officer erhält das Recht, den Namen dieses Security Officers ändern zu dürfen.
Zertifikat ändern	Der hinzugefügte Security Officer erhält das Recht, das Zertifikat dieses Security Officers ändern zu dürfen.
Region ändern	Der hinzugefügte Security Officer erhält das Recht, die Zuweisung der Region (Präfix) dieses Security Officers ändern zu dürfen.
Konfiguration zuordnen	Der hinzugefügte Security Officer erhält das Recht, die Konfiguration (bearbeiten und zuordnen der Pfade) dieses Security Officers ändern zu dürfen.
Security Officer löschen	Der hinzugefügte Security Officer erhält das Recht, diesen Security Officer löschen zu dürfen.
Globale Rechte ändern	Der hinzugefügte Security Officer erhält das Recht, die Einstellungen für die globalen Rechte dieses Security Officers ändern zu dürfen.
ACL ändern	Der hinzugefügte Security Officer erhält das Recht, die ACL dieses Security Officers ändern zu dürfen.
Lesen	Der hinzugefügte Security Officer erhält das Recht, sich diesen Security Officer anzeigen zu lassen. Dieser wird ihm dann nach seiner Anmeldung an der *u.trust LAN Crypt*-Admin-Konsole unter **Zentrale Einstellungen / Security Officer Administration** angezeigt. Wenn dieses Recht nicht erteilt wurde, können auch alle weiteren Rechte, die eine Bearbeitung von Security Officer durch einen anderen Security Officer ermöglichen, nicht ausgeführt werden. Dieses Recht wird aus diesem Grund automatisch gesetzt, sobald einem Security Officer irgendein Recht zum Bearbeiten der Einstellungen eines anderen Security Officers übertragen wurde.

5.2.3 Rechte zur Bearbeitung von Gruppen

Rechte	Beschreibung
Schlüssel erzeugen	Der Security Officer darf Schlüssel in der Gruppe erzeugen.
Schlüssel kopieren	Der Security Officer darf Schlüssel kopieren.
Schlüssel entfernen	Der Security Officer darf Schlüssel entfernen.
Regeln erzeugen	Der Security Officer darf Verschlüsselungs-regeln erzeugen.
Zertifikate zuweisen	Der Security Officer darf den Benutzern Zertifikate zuweisen. Der Security Officer ist dazu berechtigt, den Assistenten für das Zuweisen von Zertifikaten auszuführen. Diese Berechtigung erlaubt es dem Security Officer, den Benutzern in der Gruppe Zertifikate zuzuweisen, wenn die Gruppe auch die übergeordnete Gruppe ist.
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung **Zertifikate zuweisen** gesetzt ist. **Zertifikate allen Mitgliedern zuweisen** berechtigt einen Security Officer zum Zuweisen von Zertifikaten zu Benutzern, wenn der Security Officer die Berechtigung **Zertifikate zuweisen** für die übergeordnete Gruppe des Benutzers oder die Berechtigung **Zertifikate allen Mitgliedern zuweisen** für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung **Zertifikate zuweisen** eine Voraussetzung für **Zertifikate allen Mitgliedern zuweisen** ist, gilt: Wenn Sie die Berechtigung **Zertifikate zuweisen** deaktivieren, wird auch die Berechtigung **Zertifikate allen Mitgliedern zuweisen** deaktiviert.
Benutzer hinzufügen	Der Security Officer darf manuell Benutzer zur Gruppe hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.

Rechte	Beschreibung
Benutzer kopieren	Der Security Officer darf Benutzer zu Gruppen hinzufügen (kopieren). Dies ist nur denjenigen Mitgliedern erlaubt, für die diese Gruppe auch das übergeordnete Objekt ist.
Benutzer löschen	Der Security Officer darf Benutzer über das Snap-In *Mitglieder und Zertifikate für Gruppe* löschen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Gruppe hinzufügen	Der Security Officer darf über das Kontext-menü einer Gruppe neue Gruppen hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Untergruppe entfernen	Der Security Officer darf Untergruppen dieser Gruppe entfernen. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Gruppen verschieben	Der Security Officer darf manuell angelegte Gruppen in der Administration (mit „*Drag & Drop*“) verschieben. Importierte Gruppen können nicht verschoben werden. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.
Eigenschaften ändern	Der Security Officer darf die Eigenschaften der Gruppe ändern.
Gruppe löschen	Der Security Officer darf Gruppen löschen. Dies setzt voraus, dass er in der übergeordneten Gruppe das Recht **Untergruppe entfernen** hat. Dieses Recht ist eine Voraussetzung für das Importieren / Synchronisieren von Gruppen und Benutzern.

Rechte	Beschreibung
Profile erzeugen	Der Security Officer darf den Profile Resolver starten und Profildateien für ausgewählte Benutzer erstellen. **Profile erzeugen** berechtigt den Security Officer, Profile für Benutzer zu erstellen, für die die Gruppe auch die übergeordnete Gruppe ist.
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung **Profile erzeugen** gesetzt ist. **Profile für alle Mitglieder erzeugen** berechtigt den Security Officer dazu, Profile für alle Benutzer in der Gruppe zu erzeugen: Benutzer, für die die Gruppe auch die übergeordnete Gruppe ist, und Benutzer, die Mitglieder der Gruppe sind, jedoch eine andere übergeordnete Gruppe haben. **Hinweis:** Wenn Sie *Profile für alle Mitglieder erzeugen* auf **Zulassen** setzen, wird die Berechtigung *Profile erzeugen* automatisch auf **Zulassen** gesetzt. Wenn Sie *Profile erzeugen* auf **Verweigern** setzen, wird die Berechtigung *Profile für alle Mitglieder erzeugen* automatisch auf **Verweigern** gesetzt.
ACL ändern	Der Security Officer darf die ACL dieser Gruppe ändern (z. B. einen anderen Security Officer hinzufügen).
Lesen	Der Security Officer hat Leserechte an dieser Gruppe, er kann den Inhalt der Snap-Ins sehen. Wird automatisch gesetzt, wenn Bearbeitungsrechte vergeben werden.
Sichtbar	Die Gruppe ist für den Security Officer sichtbar. Wird am Basisknoten gesetzt und nach unten vererbt. Wird es dem Security Officer verweigert, wird die Gruppe ausgeblendet (auch das globale Recht **Lesen** muss verweigert sein).

6 Rechtlicher Hinweis

7 Technischer Support

Technischen Support zu u.trust LAN Crypt können Sie wie folgt abrufen:

- Unter https://support.hsm.utimaco.com erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie beispielsweise Knowledge-Items.

Die Dokumentation *zu u.trust LAN Crypt*-Client für Windows erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/windows/13_0_1/de/
- in englischer Sprache: https://help.lancrypt.com/docs/windows/13_0_1/en/
- in französischer Sprache: https://help.lancrypt.com/docs/windows/13_0_1/fr/

Die Dokumentation zu *u.trust LAN Crypt*-Client für macOS erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/macOS/de/
- in englischer Sprache: https://help.lancrypt.com/docs/macOS/en/

Die Dokumentation zu *u.trust LAN Crypt für iOS / iPadOS* erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/ios/de/
- in englischer Sprache: https://help.lancrypt.com/docs/ios/en/

Die Dokumentation zu *u.trust LAN Crypt für Android* erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/android/de/
- in englischer Sprache: https://help.lancrypt.com/docs/android/en/

Die Dokumentation zu *u.trust LAN Crypt 2Go* erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/2Go/de/
- in englischer Sprache: https://help.lancrypt.com/docs/2Go/en/

Die Dokumentation zu *u.trust LAN Crypt*-Admin erhalten Sie zum Herunterladen

- in deutscher Sprache: https://help.lancrypt.com/docs/admin/13_0_1/de/
- in englischer Sprache: https://help.lancrypt.com/docs/admin/13_0_1/en/
- in französischer Sprache: https://help.lancrypt.com/docs/admin/13_0_1/fr/
- in japanischer Sprache: https://help.lancrypt.com/docs/admin/13_0_1/jp/

Als Wartungsvertragskunde senden Sie eine E-Mail an den technischen Support:

support@utimaco.com

und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch-Level Ihrer *u.trust LAN Crypt* Software sowie ggf. den genauen Wortlaut von Fehlermeldungen ergänzend mit an.