conpal LAN Crypt

Persistent
Hochsicher
Skalierbar

macOS

Produktversion: 1.0.0
Stand: Juli 2021

INHALT

1 Was ist conpal LAN Crypt?

conpal LAN Crypt ermöglicht mit transparenter Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in kleinen, mittleren und großen Organisationen. *conpal LAN Crypt* funktioniert ohne Benutzerinteraktion. Es unterstützt die Rolle eines Security Officers (SO), der die Zugriffsrechte auf Dateien, die mit *conpal LAN Crypt* verschlüsselt sind, einschränken kann. Ein Master Security Officer (MSO) hat das Recht, *conpal LAN Crypt* zu verwalten oder auch Berechtigungen zu delegieren. Auf diese Weise lässt sich auch eine Hierarchie von Security Officern einrichten, die die Sicherheitsanforderungen in jedem Unternehmen erfüllen kann.

Verschlüsselte Dateien müssen nicht einzelnen Benutzern zugewiesen sein. Jeder Benutzer, der über den erforderlichen Schlüssel verfügt, kann mit einer verschlüsselten Datei arbeiten. Dies erlaubt Administratoren das Erzeugen von logischen Benutzergruppen, die gemeinsam auf verschlüsselte Dateien zugreifen und mit diesen arbeiten können. Dieser Vorgang kann mit einer Art Schlüsselbund, wie er im täglichen Leben verwendet wird, verglichen werden. *conpal LAN Crypt* stattet Benutzer und Benutzergruppen mit einem Schlüsselbund aus, dessen einzelne Schlüssel für verschiedene Ordner oder Dateien verwendet werden können.

Jedes Mal, wenn ein Benutzer eine Datei in einen verschlüsselten Ordner verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt. Wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Ordner liest, wird sie in verschlüsselter Form übertragen. Die Datei wird nur auf dem Computer des Empfängers entschlüsselt. Der Benutzer kann sie dort bearbeiten. Bevor die Datei wieder in den verschlüsselten Ordner übertragen wird, wird sie wieder verschlüsselt.

Nicht berechtigte Benutzer können unter Umständen auf diese verschlüsselten Dateien zugreifen (nur von Arbeitsstationen ohne *conpal LAN Cryp*t), sehen aber ohne die entsprechende *conpal LAN Crypt* Berechtigung nur deren verschlüsselten Inhalt.

1.1 Schutz von Daten durch *conpal LAN Crypt*

conpal LAN Crypt garantiert, dass sensible Dateien verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da die Ver- und Entschlüsselung im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen transparent und weitgehend ohne Benutzerinteraktionen ab. Auf dem Datei-Server selbst muss keine spezielle Sicherheitssoftware installiert werden.

Ein Security Officer kann unterschiedliche Zugriffsrechte für Ordner und Dateien definieren. Diese Rechte werden in Verschlüsselungsprofilen für die Benutzer zusammengefasst. Verschlüsselungsprofile werden über Richtliniendateien an die Benutzer verteilt. Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden. Die Richtliniendatei ist durch ein Zertifikat geschützt. Damit Benutzer auf ihren Computern Dateien verarbeiten können, die mit *conpal LAN Crypt* verschlüsselt sind, müssen sie Zugriff auf die Richtliniendatei haben. Durch den Besitz des zum Zertifikat gehörenden privaten Schlüssels hat der Benutzer Zugriff auf die Richtliniendatei, in der das Verschlüsselungsprofil gespeichert ist.

conpal LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen. Alle *conpal LAN Crypt* Benutzer, die in ihrer Richtliniendatei dasselbe Verschlüsselungsprofil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Sie brauchen sich nicht um die Verschlüsselung oder um den Schlüsselaustausch kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen, damit die Dateien transparent ver- bzw. entschlüsselt werden können, sobald sie geöffnet bzw. geschlossen werden. Es können alle Organisationsformen abgebildet werden - von einem LAN-Modell, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer nur Notebooks einsetzen.

1.2 Unterschiede von conpal LAN Crypt für Windows und macOS

Konfigurationsdatei ersetzt Gruppenrichtliniendatei

Die Clientversion von *conpal LAN Crypt für macOS* verfügt in Version 1.0.0 über kein Benutzermenü. Sämtliche Einstellungen erfolgen über die Datei `config.plist`, die nach der Installation zu erstellen ist (siehe „Konfigurationsdatei erstellen“) auf Seite 7.

Die Erstellung einer Konfigurationsdatei ist notwendig, da der mac-Client selbst keine Gruppenrichtlinien von Windows verwenden kann. Die Konfigurationsdatei enthält daher alle für den mac-Client erforderlichen Einstellungen, wie z. B. die Pfadangaben, in denen die Richtliniendatei, das öffentliche Zertifikat des Security Officers und auch die Schlüsseldatei des Benutzers gespeichert sind.

Von *conpal LAN Crypt für macOS* unterstützte Verschlüsselungsalgorithmen

conpal LAN Crypt für macOS unterstützt folgende Verschlüsselungsalgorithmen:

- AES-256 Bit (XTS-Modus)
- AES-256 Bit (CBC-Modus)
- AES-128 Bit (XTS-Modus)
- AES-128 Bit (CBC-Modus)

Hinweis: Bitte beachten Sie in diesem Zusammenhang, das *conpal LAN Crypt* für Windows auch noch weitere Verschlüsselungsalgorithmen (wie z. B. „IDEA“ oder „3DES“, etc.) unterstützt. Wenn durch den Security Officer Verschlüsselungsregeln erstellt werden, die (auch) für *conpal LAN Crypt für macOS* gelten sollen, dürfen nur die o. a. AES-Verschlüsselungsalgorithmen verwendet werden.

Wurde durch den (Master) Security Officer die Option „*Key-Wrapping*“ aktiviert (Standardeinstellung), 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.

conpal LAN Crypt für macOS unterstützt folgende Verschlüsselungsalgorithmen für das Key-Wrapping:

- AES-256 Bit
- 3DES

Hinweis: Wenn Sie Sicherheitstoken oder Smartcards verwenden, stellen Sie bitte 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.

2 Verschlüsselung

2.1 Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (in verschlüsselten Ordnern auf Netzwerkfreigaben) automatisch im Hauptspeicher entschlüsselt, sobald sie von einer Anwendung (wie z. B. von Office) geöffnet werden. Beim Speichern der Datei wird sie automatisch wieder verschlüsselt. Von der transparenten Verschlüsselung werden alle Dateivorgänge erfasst. Da alle Prozesse im Hintergrund laufen, bemerken Benutzer nichts davon, wenn sie mit verschlüsselten Dateien arbeiten.

Hinweis: *conpal LAN Crypt für macOS* Version 1.0.0 kann derzeit keine lokalen Dateien auf dem Apple-Rechner selbst ver- oder entschlüsseln. *conpal LAN Crypt für macOS* kann Dateien auf SMB-Freigaben ver- und entschlüsseln. Alle Laufwerke, auf denen Dateien ver- oder entschlüsselt werden, müssen zuvor auf dem Apple-Rechner eingebunden werden. Mithilfe des Finder-Fensters können Sie die gewünschten Laufwerke bzw. SMB-Freigaben einbinden (mounten).

Die Verschlüsselung ist nicht von Ordnern abhängig, sondern nur von Verschlüsselungsregeln. Die Verschlüsselung funktioniert wie folgt:

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden automatisch verschlüsselt.
- Werden Dateien in einen verschlüsselten Ordner verschoben oder kopiert, werden sie gemäß der für diesen Ordner definierten Verschlüsselungsregel verschlüsselt. Der Security Officer kann über die *conpal LAN Crypt* Administration mehrere Verschlüsselungsregeln für unterschiedliche Dateitypen oder Dateinamen definieren, die sich im selben Ordner befinden. Sie können so beispielsweise Worddateien mit einer anderen Regel verschlüsseln als Exceldateien, obwohl sich beide Dateien im selben Ordner befinden.
- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Wenn ein Benutzer verschlüsselte Dateien in einen anderen Ordner innerhalb derselben SMB-Freigabe oder auf eine andere SMB-Freigabe kopiert, für die keine Verschlüsselungsregel existiert, werden die Dateien automatisch entschlüsselt. Dagegen bleiben die Dateien beim Verschieben innerhalb derselben SMB-Freigabe weiterhin verschlüsselt. **Das gilt dann auch für Ordner, für die eine „*Ignorieren*“- oder „*Ausschließen*“-Regel besteht** (siehe Administrator-Handbuch, im Abschnitt „Erzeugen von Verschlüsselungsregeln“).

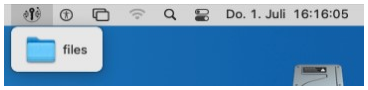
2.1.1 Zugriff auf verschlüsselte Dateien

Um verschlüsselte Dateien lesen oder schreiben zu können, benötigt ein Benutzer immer den hierfür erforderlichen Schlüssel. Alle Schlüssel und Verschlüsselungsregeln werden dem Benutzer durch den Security Officer über seine Profilrichtlinie zugewiesen.

Besitzt der Benutzer den erforderlichen Schlüssel, mit dem Dateien verschlüsselt sind, kann er sie grundsätzlich öffnen. Das gilt insbesondere auch dann, wenn in der Profilrichtlinie für eine SMB-Freigabe und für die dort vorhandenen Verzeichnissen sowie Dateien keine Verschlüsselungsregel besteht.

Hinweis: Besteht für eine SMB-Freigabe eine „*Ignorieren-Regel*“, kann ein Benutzer dort enthaltene verschlüsselte Dateien jedoch nicht öffnen, auch wenn dieser den hierfür erforderlichen Schlüssel besitzen sollte.

Wenn Sie im Schnellzugriff auf Ihre verschlüsselten Dateien zugreifen wollen, können sie oben rechts auf Ihrem Desktop auf das Schlüsselsymbol von *conpal LAN Crypt für macOS* klicken. Klicken Sie dann auf die dort angezeigten Ordner. Hierbei werden alle verschlüsselten SMB-Freigaben gelistet und können kurze Zeit später (nach ca. 30 Sekunden) von Ihnen geöffnet werden.



2.1.2 Explizite Entschlüsselung von Dateien

Um eine Datei zu entschlüsseln, müssen Sie diese nur in einen Ordner ohne Verschlüsselungsregeln kopieren oder verschieben. Die Datei wird dann automatisch entschlüsselt. Voraussetzungen:

- Ein entsprechendes Verschlüsselungsprofil ist geladen,
- der Benutzer verfügt über den erforderlichen Schlüssel
- und das aktive Verschlüsselungsprofil enthält keine Verschlüsselungsregel für den neuen Speicherort.

2.1.3 Von der Verschlüsselung ausgenommene Dateien und Ordner

Folgende Dateien und Ordner sind automatisch von der Verschlüsselung ausgenommen, auch wenn für sie eine Verschlüsselungsregel definiert wurde:

- Dateien auf allen lokalen Laufwerken.
- Dateien in Ordnern, die in *conpal LAN Crypt* mit einer „*Ausnahme*“- oder „*Ignorieren*“-Regel definiert sind.

2.2 Transparente Verschlüsselung und Komprimierungsprogramme

Komprimierungsprogramme öffnen Dateien, lesen deren Inhalte und erzeugen hieraus eine komprimierte Archivdatei. Die gepackten Archivdateien können mithilfe des Komprimierungsprogramms jederzeit wieder entpackt werden. Auf diese Weise lassen sich die ursprünglichen Dateien an jedem beliebigen Ort wiederherstellen. Wenn die transparente Ent-/Verschlüsselung aktiviert ist, erhalten diese Programme die entschlüsselten Dateien und diese werden dann komprimiert. Die Dateien im Archiv selbst sind dann nicht mehr mit *conpal LAN Crypt* verschlüsselt. Wird das Archiv an einem Ort bzw. in einem Ordner gespeichert, für den keine Verschlüsselungsregel existiert, dann sind alle Dateien im Klartext und damit unverschlüsselt.

3 Konfiguration

3.1 Konfigurationsdatei erstellen

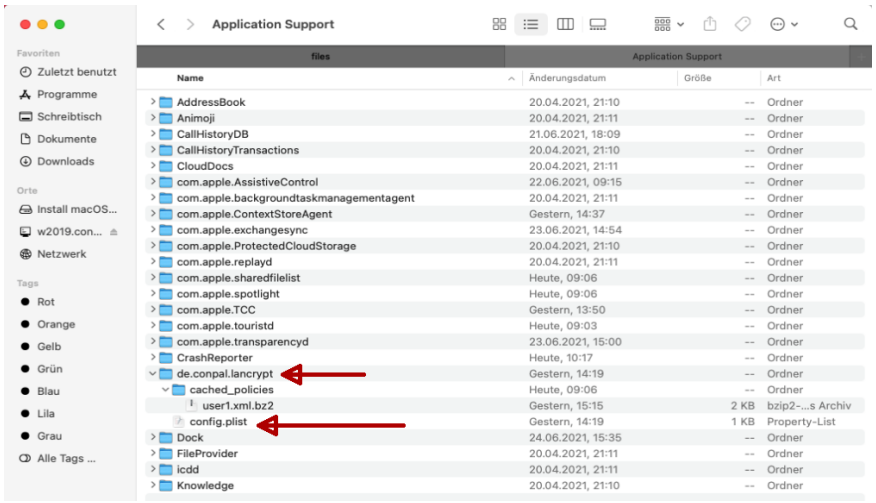
Sämtliche Einstellungen *für conpal LAN Crypt für macOS* erfolgen über die Konfigurationsdatei `config.plist`, die nach der Installation zu erstellen ist. Diese enthält alle für *conpal LAN Crypt für macOS* erforderlichen Einstellungen, wie z. B. die Pfadangaben, in denen die Richtliniendateien (*.bz2*), die öffentlichen Zertifikate (*.cer*) der (Master)Security Officer und die Schlüsseldateien der Benutzer (*.p12*) gespeichert sind, sodass *conpal LAN Crypt für macOS* diese finden kann. Für die leichtere Erstellung wird ein PLIST-Template mitgeliefert und in folgendem Verzeichnis installiert:

```
/Library/conpal/LAN Crypt/useragent.app/Contents/Resources/config.plist.template
```

Es wird empfohlen, dieses Template File als Vorlage zu nehmen und die einzelnen Optionen den Anforderungen gemäß anzupassen.

Diese Datei muss nach der Erstellung in den Ordner

```
~/Library/Application Support/de.conpal.lancrypt/
```



kopiert werden.

Die Konfigurationsdatei von *conpal LAN Crypt für macOS* ist wie folgt aufgebaut:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
    <dict>
        <!-- Mandatory; Mountpoint for a share where policies are located -->
        <key>PolicyPath</key>
        <string>/Volumes/share/policies</string>

        <!-- Mandatory; Mountpoint for a share where the SO certificate is located -->
        <key>SOCertLocation</key>
        <string>/Volumes/share/keys</string>

        <!-- Optional; Only needed if the username on the machine differs from the username in the policy -->
        <key>UserName</key>
        <string>LANCryptUser</string>

        <!-- Optional; Mountpoint for a share where certificates are located -->
        <key>CertificatePath</key>
        <string>/Volumes/share/keys</string>

        <!-- Optional; When set to true, for every connected network share a mountpoint will be created -->
        <key>AutoMountAllNetworkShares</key>
        <true/>

        <!-- Optional; When set to true, certificates will not be validated -->
        <key>DisableCertificateValidation</key>
        <false/>

        <!-- Optional; Additional keywords used when expanding keywords in the policy -->
        <key>AgentEnvironment</key>
        <dict>
            <!-- will expand %custom_key% in rule to custom_value -->
            <key>custom_key</key>
            <string>custom_value</string>
        </dict>
    </dict>
</plist>
```

3.1.1 Einträge in der Konfigurationsdatei

1. Mountpoint zur Richtliniendatei (<key>Policypath<key>)

Tragen Sie im Abschnitt <*string*> die Freigabe ein, unter der die Richtliniendateien (*.xml.bz2)* der Benutzer gespeichert sind.

Beispiel:

```
<key>Policypath<key>
<string>/Volumes/lancrypt/Profile</string>
```

2. Mountpoint zum öffentlichen Zertifikat des Security Officers (<key>SOCertLocation</key>)

Tragen Sie im Abschnitt <*string*> die Freigabe ein, unter der die öffentlichen Zertifikate (*.cer*) der Security Officer gespeichert sind.

Beispiel:

```
<key>SOCertLocation</key>
<string>/Volumes/lancrypt/Zertifikate</string>
```

Hinweis: Die Mountpoints zur Richtliniendatei und zum öffentlichen Zertifikat (*.cer*) des Security Officers müssen unbedingt in die Konfigurationsdatei eingetragen werden.

Optionale Einstellungen der Konfigurationsdatei

Sie können darüber hinaus auch noch weitere optionale Einstellungen in der in der Konfigurationsdatei vornehmen. Solche Angaben sind dann wichtig, wenn beispielsweise der Benutzeranmeldename beim mac-Rechner sich vom Benutzernamen in der *conpal LAN Crypt* Administration unterscheiden sollte.

3. Anmeldename des Benutzers (<key>UserName</key>)

Dem Attribut für den Anmeldenamen kommt eine besondere Bedeutung zu. *conpal LAN Crypt* benennt die Richtliniendateien nach dem Anmeldenamen der Benutzer. Nur wenn der Anmeldename und der Name der Richtliniendatei identisch sind, kann sich der Benutzer bei *conpal LAN Crypt für macOS* anmelden. Da der Benutzeranmeldename beim mac-Rechner jedoch anders lauten könnte, müssen Sie in dem Fall in die Konfigurationsdatei den zur Richtliniendatei passenden Namen dort eintragen. Nur dann kann *conpal LAN Crypt für macOS* die richtige Richtliniendatei laden.

4. Mountpoint zur Schlüsseldatei (.p12) des Benutzers (<key>CertificatePath</key>)

Nach Angabe des Mountpoints für die Schlüsseldatei (*.p12*) des Benutzers, versucht *conpal LAN Crypt für macOS* automatisch eine *.p12-Schlüsseldatei in den Schlüsselbund des Benutzers zu importieren, falls der private Schlüssel der Richtliniendatei nicht vorhanden ist. Diese Datei muss "*Anmeldename.p12*" heißen, damit sie für den betreffenden Benutzer erkannt wird.

Hinweis: Wenn die Anmeldung der Benutzer mit einem Sicherheitstoken oder mit einer Smartcard erfolgen soll, darf in der Konfigurationsdatei kein Mountpoint zur Schlüsseldatei (*.p12*) des Benutzers eingetragen werden.

5. Alle Netzwerkverbindungen automatisch herstellen (<key>AutoMountAllNetworkShares</key>)

Stellen Sie den dazugehörigen Parameter auf „**true**“, wird *conpal LAN Crypt für macOS* automatisch alle zurzeit verbundenen und auch alle SMB-Freigaben, die in Zukunft verbunden werden, für die transparente Dateiverschlüsselung zur Verfügung stellen.

Beispiel:

```
<key>AutoMountAllNetworkShares</key>
<true/>
```

Im Beispiel oben werden alle verfügbaren SMB-Freigaben automatisch als LCFS-Freigaben gemounted. *conpal LAN Crypt für macOS* kann dann auf diese gemounteten Freigaben zugreifen.

Hinweis: Wenn Sie den Parameter für diese Einstellung nach „**false**“ ändern, hat das zur Folge, dass Verschlüsselungsregeln, die relative Pfadangaben enthalten (z. B. `meine_daten\*.*`) nicht funktionieren. Die Pfade in Verschlüsselungsregeln müssen bei der Einstellung „**false**“ immer als absolute Pfadangaben definiert werden.

Beispiel:

```
\\server\meine_daten\*.*
```

6. Fehler bei der Zertifikatsprüfung ignorieren (<key>DisableCertificateValidation</key>)

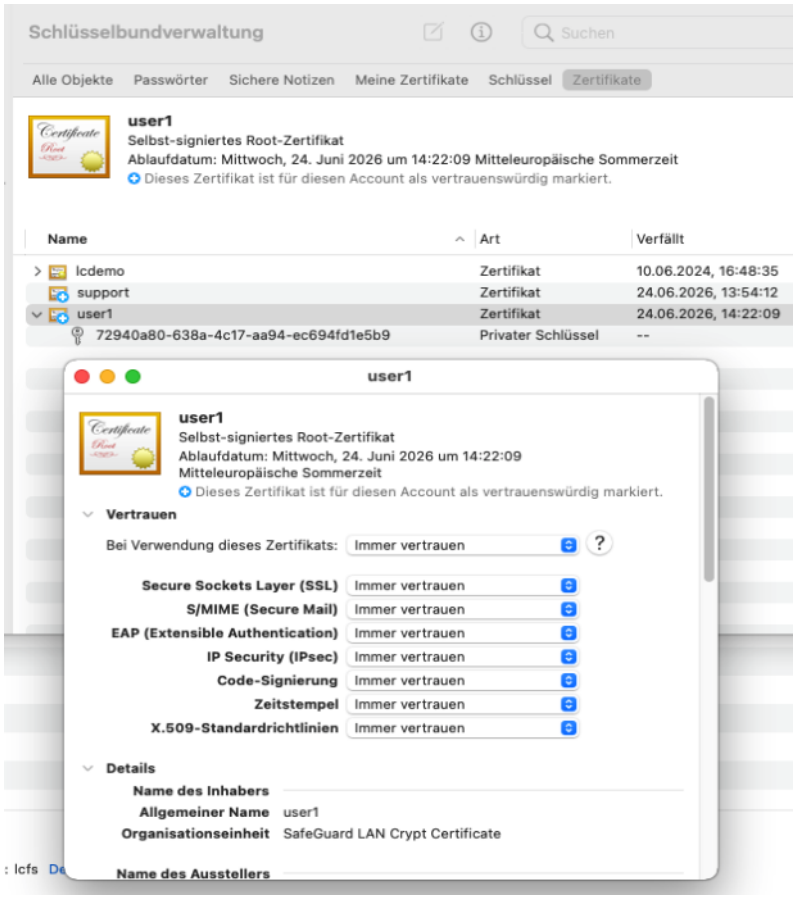
conpal LAN Crypt erlaubt festzulegen, ob mögliche Fehler bei der Überprüfung der Zertifikate der Benutzer ignoriert werden.

Beispiel:

```
<key>DisableCertificateValidation</key>
<true/>
```

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 eigentlich abgelaufenen Zertifikate noch weiterverwendet werden. Sind die neuen Zertifikate verfügbar, kann diese Einstellung wieder deaktiviert werden, indem Sie den Parameter für diese Einstellung nach „**false**“ ändern.

Hinweis: Bei einem Zertifikat können Sie alternativ auch über die Schlüsselbundverwaltung dessen Vertrauenseinstellung manuell einstellen und so beispielsweise einem Zertifikat immer vertrauen.



Hinweis: Änderungen von Vertrauenseinstellungen erfordern immer administrative Rechte.

Hinweis: Fehler bei der Zertifikatsprüfung zu ignorieren, bedeutet immer auch eine Senkung des Sicherheitsniveaus.

7. Umgebungsvariablen verwenden (<key>AgentEnvironment</key>)

Hier können Sie Umgebungsvariablen definieren, die Sie für Verschlüsselungsregeln in Richtliniendateien verwendet haben. Damit diese auch vom mac-Rechner entsprechend aufgelöst werden können, müssen Sie diesen Umgebungsvariablen die entsprechenden Werte bzw. Namen zuweisen.

Beispiel:

```
<key>AgentEnvironment</key>
<dict>
<key>%Username2%</key>
<string>harald</string>
<key>%Platzhalter1%</key>
<string>Bilanzen</string>
<key>%Platzhalter2%</key>
<string>GF</string>
</dict>
```

Hinweis: Die Anzahl der Umgebungsvariablen, die Sie im Abschnitt *<key>AgentEnvironment</key>* definieren können, ist unbegrenzt.

3.1.2 Konfigurationsdatei neu laden

Um eine geänderte Konfigurationsdatei („*config.plist*“) neu zu laden, muss der Benutzer das Terminal öffnen und dort den folgenden Befehl ausführen:

```
launchctl unload /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist
&& launchctl load /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist
```

Die geänderte Konfigurationsdatei wird danach neu geladen, ohne dass der Benutzer sich vom mac-Rechner abmelden und wieder neu anmelden oder der mac-Rechner neu gestartet werden muss.

3.2 Zertifikate

Bevor ein Benutzer Zugriff auf sein Verschlüsselungsprofil hat, muss das entsprechende Zertifikat auf seinem Computer vorhanden sein. Der Security Officer muss diese Zertifikate an die Benutzer verteilen und ihnen auch das Passwort bzw. die PIN für den Zugriff auf ihr Zertifikat mitteilen. Hierzu muss der Administrator auf dem mac-Client die Konfigurationsdatei „*config.plist*“ erstellen. Dort ist der Pfad einzutragen, in dem die *conpal LAN Crypt* Administration sowohl die Benutzerzertifikate als auch das öffentliche Zertifikat des Security Officers (*.cer) speichert (vgl. *conpal LAN Crypt* Administrations-Handbuch, „**Zentrale Einstellungen**“, „**Verzeichnisse**“). Aus diesem Pfad importieren die Benutzer dann ihre PKCS#12-Schlüsseldatei (ihr Zertifikat) auf ihren Computer. Sind die Zertifikate bereits bei der ersten Anmeldung verfügbar, läuft der gesamte Vorgang bis zur PIN-Eingabe ohne weitere Interaktion des Benutzers automatisch ab.

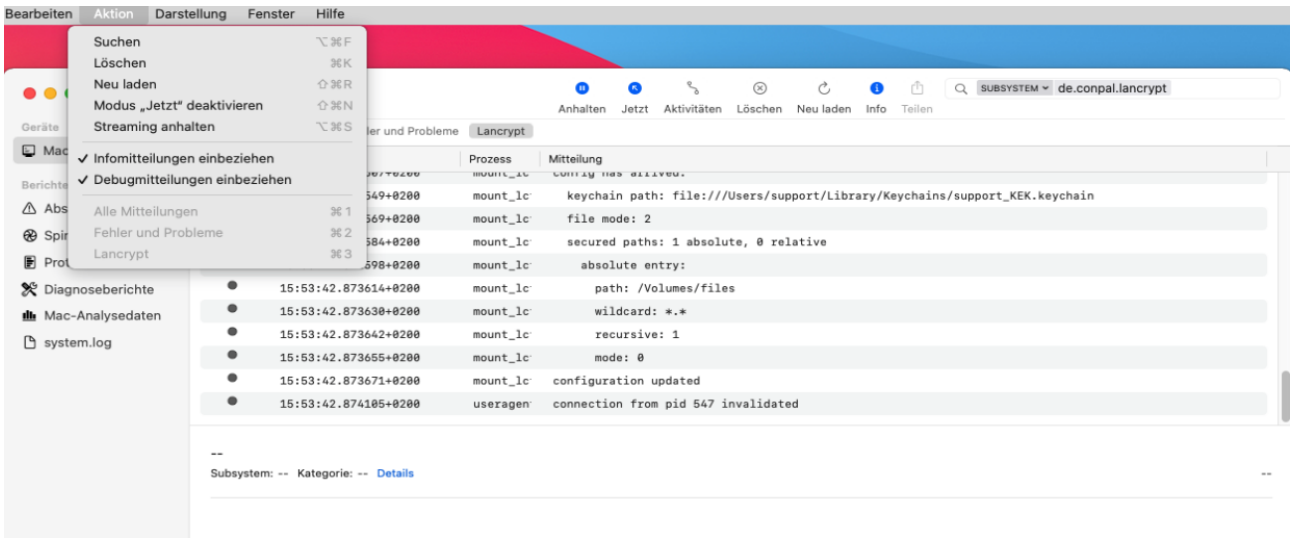
conpal LAN Crypt bietet die Möglichkeit, die Zertifikate beim ersten Laden des Verschlüsselungsprofils automatisch zu importieren. In diesem Fall wird das System vom Security Officer so konfiguriert, dass *conpal LAN Crypt* bei der ersten Anmeldung auch eine Zertifikatsdatei findet und dann den Importvorgang automatisch durchführt. Der Benutzer wird einmal aufgefordert, die PIN für den Import der PKCS#12 Schlüsseldatei einzugeben.

Hinweis: Der Security Officer muss den Benutzern deren PIN auch beim automatischen Import ihrer Zertifikate mitteilen.

Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils geprüft. Wird ein gültiges Zertifikat gefunden, wird der Benutzer an *conpal LAN Crypt* angemeldet. Ist kein gültiges Zertifikat vorhanden, kann der Benutzer nicht mit den verschlüsselten Daten arbeiten.

Hinweis: Wenn die Anmeldung an *conpal LAN Crypt* fehlschlägt, werden diese in der mac-Konsole unter dem Filter „`subsystem de.conpal.de.lancrypt`“ in den jeweiligen Logeinträgen angezeigt. Aktivieren Sie in der Konsole auch die Optionen „*Informationsmitteilungen einbeziehen*“ sowie „*Debugmitteilungen einbeziehen*“. Alternativ können Sie sich diese Informationen auch in einem Terminal live ansehen. Hierzu ist folgende Eingabe in dem Terminal erforderlich:

```
sudo log stream --level debug --predicate 'subsystem == "de.conpal.lancrypt"'
```



Die spezifischen Verschlüsselungsregeln, die in den *conpal LAN Crypt* Verschlüsselungsprofilen enthalten sind, ermöglichen dem Benutzer den Zugriff auf verschlüsselte Dateien in den zuvor freigegebenen SMB-Shares. Diese Regeln definieren, welche Dateien in welchen Ordnern der Shares mit welchem Schlüssel zu verschlüsseln sind. Es muss nur ein Verschlüsselungsprofil eines Benutzers geladen werden, dann finden Verschlüsselung und Entschlüsselung transparent im Hintergrund statt.

Der Benutzer selbst bemerkt die durchgeführten Verschlüsselungs-/Entschlüsselungsvorgänge nicht. Die Regeln lassen sich jederzeit und beliebig durch den *conpal LAN Crypt* (Master) Security Officer (MSO/SO) ändern. So können beispielsweise auch Dateien mit einem anderen Schlüssel umgeschlüsselt werden.

3.3 Laden der Richtliniendatei

3.3.1 Standardverhalten von *conpal LAN Crypt*

Wenn sich ein Benutzer an seinem mac-Rechner anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach prüft *conpal LAN Crypt*, ob für den Benutzer eine neue Richtliniendatei verfügbar ist, indem es eine Verbindung zum festgelegten Speicherort für Richtliniendateien (SMB-Share) aufbaut. Wird eine neuere Richtliniendatei gefunden, führt dies automatisch zu einer Aktualisierung des zwischengespeicherten Benutzerprofils.

Der Benutzer kann weiterhin mit verschlüsselten Daten arbeiten, während *conpal LAN Crypt* noch überprüft, ob es eine neuere Version der Richtliniendatei gibt. Ist der für die Richtliniendatei angegebene Speicherort nicht erreichbar, arbeitet der Benutzer dann solange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

Hinweis: *conpal LAN Crypt* verifiziert die Zertifikate der Benutzer und das öffentliche Zertifikat vom (Master) Security Officer (.cer), der die Richtliniendatei erstellt hat. Enthält ein Zertifikat einen „CRL Distribution Point“ und es ist keine gültige CRL auf dem System verfügbar, vertraut *conpal LAN Crypt für macOS* diesem Zertifikat zunächst nicht. Im Schlüsselbund des Benutzers kann der Benutzer die Vertrauenseinstellung ändern und dort für dieses Zertifikat dann die Einstellung „immer vertrauen“ zuweisen.

3.3.2 Aktualisierte Richtliniendatei manuell laden

Durch den Security Officer erhält der Benutzer seine Richtliniendatei. Wird diese Richtliniendatei durch den Security Officer aktualisiert, wird diese aktualisierte Version erst geladen, wenn der Benutzer sich bei seinem mac-Rechner abmeldet und danach wieder anmeldet bzw. seinen Rechner neu startet. In manchen Fällen kann es aber sinnvoll sein, dass der Benutzer seine aktualisierte Richtliniendatei auch aktualisieren kann, ohne sich abmelden zu müssen.

Hierzu muss der Benutzer auf seinem mac-Rechner das Terminal öffnen und dort dann den folgenden Befehl ausführen:

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil reload-policies
```

Nach dem Ausführen dieses Befehls wird die Richtliniendatei des Benutzers neu geladen.

3.4 Anmeldung an *conpal LAN Crypt*

conpal LAN Crypt Verschlüsselungsprofile werden von einem Security Officer entsprechend der firmenweiten Sicherheitspolitik für die Benutzer erstellt und in Richtliniendateien gespeichert. Ein Verschlüsselungsprofil kann nur geladen werden, wenn der Benutzer auch über das hierfür erforderliche Zertifikat verfügt.

Gespeichert werden die Richtliniendateien in einem hierfür definierten Pfad (Netzwerkfreigabe). Damit *conpal LAN Crypt für macOS* die Richtliniendatei finden kann, muss dieser Pfad auch in der Konfigurationsdatei eingetragen sein. Dies gilt auch für den Pfad in dem das öffentliche Zertifikat des Security Officers zu finden ist.

Wenn sich ein Benutzer an *conpal LAN Crypt* anmeldet, wird das Verschlüsselungsprofil, das in der Richtliniendatei gespeichert ist, vom *conpal LAN Crypt für macOS-Rechner* geladen. *conpal LAN Crypt* lädt die Richtliniendatei aus der angegebenen SMB-Freigabe und prüft anhand des Benutzerzertifikats, ob der Benutzer berechtigt ist, diese zu laden.

3.4.1 Anmeldung mit Sicherheitstoken

Benutzer können für die Anmeldung an *conpal LAN Crypt für macOS* auch einen Sicherheitstoken verwenden. Voraussetzung dafür ist, dass das *conpal LAN Crypt* Benutzerzertifikat auf dem Token gespeichert ist. Wird das Benutzerzertifikat auf einem mit dem System verbundenen Token gefunden, wird die Anmeldung durchgeführt.

Hinweis: Wenn die Anmeldung der Benutzer mit einem Sicherheitstoken oder mit einer Smartcard erfolgen soll, darf in der Konfigurationsdatei kein Mountpoint zur Schlüsseldatei (*.p12*) des Benutzers eingetragen sein.

4 Installation

Hinweis: Für die Installation von *conpal LAN Crypt* für macOS benötigen Sie Administratorrechte.

conpal LAN Crypt für macOS unterstützt folgende Versionen in deutscher und englischer Sprache von macOS:

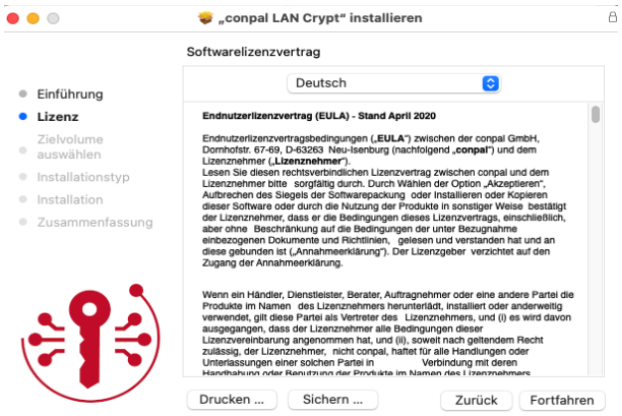
- v11 Big Sur
- v10.15 Catalina
- v10.14 Mojave

Doppelklicken Sie auf die Datei **conpal LAN Crypt.dmg**.

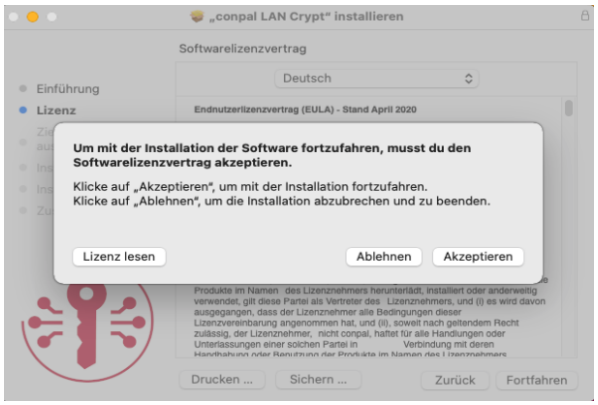
Der folgende Dialog wird angezeigt:

Doppelklicken Sie auf **conpal LAN Crypt.pkg**.

Der Dialog **Lizenzvertrag** wird angezeigt.



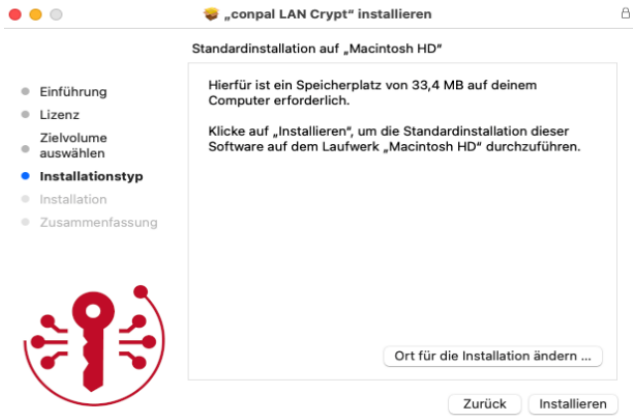
Klicken Sie auf **Fortfahren**.



Klicken Sie dann auf **Akzeptieren**.

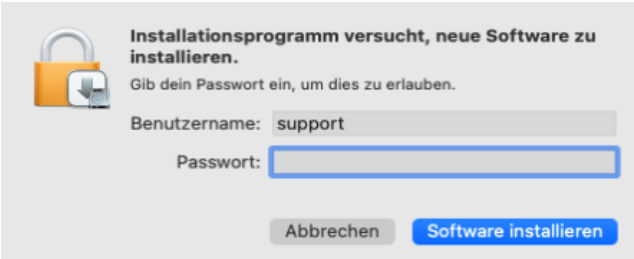
Hinweis: Wenn Sie den Softwarelizenzvertrag nicht akzeptieren und auf **Ablehnen** drücken, kann *conpal LAN Crypt für macOS* nicht installiert werden.

Wenn Sie den Softwarelizenzvertrag akzeptiert haben, wird folgender Dialog angezeigt:



Klicken Sie auf **Installieren**.

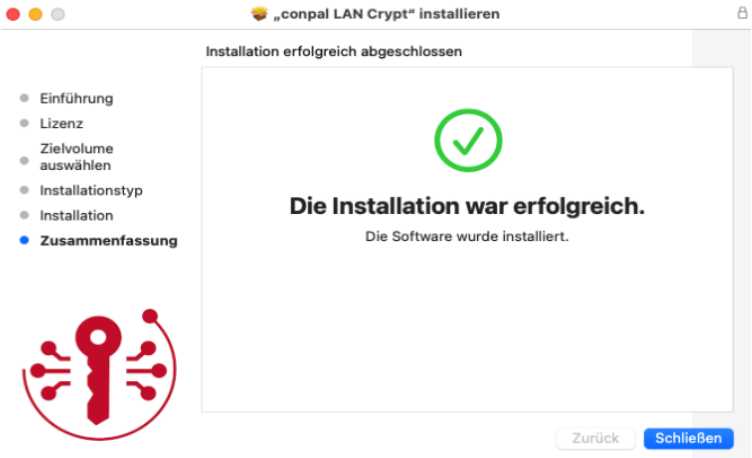
Sie erhalten die Warnmeldung, dass ein Installationsprogramm versucht, neue Software zu installieren:



Melden Sie sich als Administrator mit Ihrem dazugehörigen Benutzername und Ihrem Passwort an, und klicken Sie auf **Software installieren**.

conpal LAN Crypt für macOS wird dann auf ihrem mac-Rechner installiert.

Ist die Installation erfolgreich, so erscheint ein Dialog, in dem Sie auf **Schließen** klicken können, um den Installationsprozess abzuschließen.



4.1 *conpal LAN Crypt* für macOS deinstallieren

Sie können den *conpal LAN Crypt* Client nur entfernen, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind.

Klicken Sie im u. a. Pfad auf **Uninstaller.pkg**.

```
/Library/conpal/LAN Crypt/Uninstaller.pkg
```

conpal LAN Crypt für macOS wird deinstalliert.

Hinweis: Nach der Deinstallation von *conpal LAN Crypt* können auf dem mac-Rechner keine verschlüsselten Dateien mehr entschlüsselt werden. Die Deinstallation von *conpal LAN Crypt für macOS* führt nicht zu einer Entschlüsselung von Dateien.

5 Funktionen von „*lcutil*“

Zusätzlich zu den Programmkomponenten wird eine Konsolen-Applikation „`lcutil`“ installiert, die bei der Lösung technischer Probleme behilflich sein kann. Sie wird in folgendem Verzeichnis installiert:

```
/Library/conpal/LAN Crypt/useragent.app/Contents/Resources
```

Hierüber stehen den Benutzern erweiterte Funktionen von *conpal LAN Crypt für macOS* zur Verfügung gestellt, die im Folgenden beschrieben werden:

5.1 Version von *conpal LAN Crypt für macOS* anzeigen lassen

Um sich die Version von *conpal LAN Crypt für macOS* anzeigen zu lassen, muss der Benutzer das Terminal öffnen und dort den folgenden Befehl ausführen:

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil version
```

5.2 Protokolldatei erstellen

Mit *conpal LAN Crypt für macOS* kann der Benutzer mithilfe des Tools „`lcutil`“ eine Protokolldatei erstellen. Bestimmte Ereignisse lassen sich auf diese Weise festhalten, auswerten, archivieren und jederzeit überprüfen.

Die Protokolldatei kann der Benutzer auf seinem mac-Rechner erstellen, indem dieser das Terminal öffnet und dort den folgenden Befehl ausführt:

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil collect-logs
```

Die folgenden Ereignisse werden hierbei in die Protokolldatei geschrieben:

- System log,
- mount table,
- process table,
- version information,
- system profiler,
- cached policies and
- config.plist

6 Technischer Support

Technischen Support zu conpal-Produkten können Sie wie folgt abrufen:

- Unter https://support.conpal.de erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie beispielsweise Knowledge-Items.

Die Dokumentation *zu conpal LAN Crypt*-Client erhalten Sie zum Herunterladen

- in deutscher Sprache: https://docs.lancrypt.com/de/client/lc_400_hdeu.pdf
- in englischer Sprache: https://docs.lancrypt.com/en/client/lc_400_heng.pdf
- in französischer Sprache: https://docs.lancrypt.com/fr/client/lc_400_hfra.pdf

Die Dokumentation zu *conpal LAN Crypt*-Client für macOS erhalten Sie zum Herunterladen

- in deutscher Sprache: https://docs.lancrypt.com/de/client/lc_macOS_100_hdeu.pdf
- in englischer Sprache: https://docs.lancrypt.com/en/client/lc_macOS_100_heng.pdf

Die Dokumentation zu *conpal LAN Crypt*-Admin erhalten Sie zum Herunterladen

- in deutscher Sprache: https://docs.lancrypt.com/de/admin/lc_401_ahdeu.pdf
- in englischer Sprache: https://docs.lancrypt.com/en/admin/lc_401_aheng.pdf
- in französischer Sprache: https://docs.lancrypt.com/fr/admin/lc_401_ahfra.pdf

Als Wartungsvertragskunde senden Sie eine E-Mail an den technischen Support:

support@conpal.de

und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch-Level Ihrer conpal Software sowie ggf. den genauen Wortlaut von Fehlermeldungen ergänzend mit an.

7 Rechtliche Hinweise