Was ist u.trust LAN Crypt 2Go Reader?

u.trust LAN Crypt 2Go Reader ermöglicht den sicheren Austausch vertraulicher Daten durch das entschlüsseln passwortgeschützter Daten.

u.trust LAN Crypt 2Go Reader ist eine Ergänzung zu den *u.trust LAN Crypt* Clients. Die Anwendung ermöglicht das einfache Entschlüsseln aller durch LAN Crypt passwortverschlüsselten Dateien, sodass Dateien auch von Personen und Organisationen, welche noch nicht eines der LAN Crypt Produkte nutzen, einfach entschlüsselt werden können.

u.trust LAN Crypt 2Go Reader ist in deutscher und englischer Sprache verfügbar.

Hinweis

- *u.trust LAN Crypt 2Go Reader* ist eng verwandt mit dem LAN Crypt 2Go Client, unterstützt aber nur die Entschlüsselung von Dateien!
- Beide Produkte (*u.trust LAN Crypt 2Go* und *u.trust LAN Crypt 2Go Reader*) können unabhängig voneinander installiert und deinstalliert werden.

Anwendungsbeispiel

Stellen Sie sich vor, Sie möchten einer externen Marketingagentur mehrere Excel-Dateien mit vertraulichen Finanzdaten zur Verfügung stellen, die mit einem der LAN Crypt Produkte verschlüsselt sind. Sie erhalten auch ein Passwort zum Entschlüsseln der Dateien.

Nun können Sie *u.trust LAN Crypt 2Go Reader* zum Entschlüsseln der gegebenen Dateien mit dem erhaltenen Passwort verwenden.

Installation und Upgrade

u.trust LAN Crypt 2Go Reader ist auf folgenden Plattformen verfügbar:

- **Windows 10** oder höher (x64)

Folgende Installationspakete sind für die einzelnen Plattformen verfügbar:

- **lc2go.msi** - Windows (Intel-x64)

Installation

u.trust LAN Crypt 2Go Reader unterstützt zwei verschiedene Installationsmodi: Aktueller Benutzer und alle Benutzer.

Installations-Option: Alle Benutzer

Die Installation von *u.trust LAN Crypt 2Go Reader* erfordert standardmäßig keine Administratorrechte und kann von jedem Benutzer ausgeführt werden. Wenn die Installation von einem Benutzer durchgeführt wird, wird die Anwendung so installiert, dass sie ausschließlich diesem Benutzer zur Verfügung steht. Andere Benutzerkonten auf demselben System haben keinen Zugriff auf das installierte Produkt.

Die administrative Installation von *u.trust LAN Crypt 2Go Reader* macht das Produkt für alle Benutzer verfügbar. Dazu müssen Sie das Setup im erweiterten Modus ausführen und den Parameter MSIINSTALLPERUSER überschreiben.

Führen Sie den folgenden Befehl von einem Windows-Terminal mit erhöhten Rechten aus:

```
msiexec /i lc2go.msi MSIINSTALLPERUSER=""
```

Dadurch wird das Produkt für alle Benutzer auf dem System installiert.

u.trust LAN Crypt 2Go Reader deinstallieren

u.trust LAN Crypt 2Go Reader kann jederzeit von einem System entfernt werden. Die Deinstallation folgt den standardmäßigen Verfahren zum Entfernen von Software für jede Plattform.

Note

- Nach der Deinstallation von *u.trust LAN Crypt 2Go Reader* können verschlüsselte Dateien auf dem Rechner nicht mehr entschlüsselt werden. Durch die Deinstallation von *u.trust LAN Crypt 2Go Reader* wird kein weiteres Produkt von *u.trust LAN Crypt* deinstalliert.

---

u.trust LAN Crypt Cloud Support

Die Nutzung von u.trust LAN Crypt Cloud ermöglicht es Benutzern, ihre Schlüssel sicher in der Cloud zu speichern. Dies geschieht automatisch und stellt den Zugriff auf den Schlüsselbund von allen Geräten des Benutzers bereit, auf allen Plattformen, die von *u.trust LAN Crypt 2Go Reader* unterstützt werden.

Änderungen am Schlüsselbund, sei es das Hinzufügen, Löschen oder Umbenennen eines Schlüssels, werden automatisch mit den anderen Geräten synchronisiert. Dies stellt sicher, dass der Benutzer stets Zugriff auf die aktuellsten Schlüssel hat, unabhängig davon, auf welchem Gerät er arbeitet.

An- und Abmeldung

Um sich anzumelden, tippen Sie auf das **Kontosymbol** in der oberen rechten Ecke der *u.trust LAN Crypt 2Go Reader* Anwendung und wählen Sie **Anmelden**:

Sollten Sie passwortbasierte Schlüssel im Schlüsselbund haben, wird der Benutzer um die Erlaubnis zum Hochladen der Schlüssel in die u.trust LAN Crypt Cloud gebeten. Die Erlaubnis, bestehende Schlüssel hochzuladen, ist zwingend notwendig. Wenn ein Benutzer nicht möchte, dass bestehende Schlüssel hochgeladen werden, müssen die Schlüssel vor der Anmeldung an die u.trust LAN Crypt Cloud gelöscht werden. Beachten Sie, dass Passwörter für passwortbasierte Schlüssel nicht zur u.trust LAN Crypt Cloud hochgeladen werden, daher ist die Option **Passwort anzeigen** für Schlüssel, die in der u.trust LAN Crypt Cloud gespeichert sind, nicht verfügbar.

Nach dem Klicken auf **Anmelden** öffnet sich der Standardbrowser des Benutzers, der nach den Anmeldedaten für die u.trust LAN Crypt Cloud fragt. Nach der Eingabe der Anmeldedaten wird eine Erfolgsmeldung im Browser angezeigt. Dies bestätigt, dass der Anmeldevorgang erfolgreich abgeschlossen wurde und der Benutzer nun Zugang zu seinen in der u.trust LAN Crypt Cloud gespeicherten Schlüsseln hat.

Um sich abzumelden, folgen Sie dem gleichen Verfahren, wählen Sie jedoch **Abmelden** anstatt **Anmelden**. Nach der Abmeldung haben Sie keinen Zugriff mehr auf die in der u.trust LAN Crypt Cloud gespeicherten Schlüssel, bis Sie sich erneut anmelden. Dies dient als zusätzliche Sicherheitsebene, um zu verhindern, dass Unbefugte auf Ihre Schlüssel zugreifen können.

Entschlüsseln von passwortgeschützten Dateien

Verwendung der grafischen Benutzeroberfläche

Beim Öffnen der App durch Auswahl des *u.trust LAN Crypt 2Go Reader* Programmsymbols erscheint der Entschlüsselungsdialog. Verwenden Sie die Schaltfläche **Auswählen...**, um die zu entschlüsselnde Datei auszuwählen oder ziehen Sie die gewünschte Datei hinein.

Beim Entschlüsseln einer Datei, welche durch eines der *LAN Crypt* Produkte passwortbasiert verschlüsselt worden ist, wird vorerst geprüft ob der benötigte Schlüssel schon gespeichert ist. Ist das der Fall, so wird dieser automatisch zum Entschlüsseln verwendet. Ist der benötigte Schlüssel noch nicht vorhanden, so muss das Schlüsselpasswort eingegeben werden, um die Datei erfolgreich zu entschlüsseln. Das eingegebene Passwort wird als Schlüssel gespeichert und kann für weitere Ver- und Entschlüsselungen genutzt werden.

Hinweis

- Beim Entschlüsseln einer Datei erstellt *u.trust LAN Crypt 2Go Reader* eine unverschlüsselte Kopie der Datei. Außerdem wird die ursprüngliche Dateierweiterung der Datei wiederhergestellt, indem die Dateierweiterung .pcrypt entfernt wird.

Verwenden des Kontextmenüs

u.trust LAN Crypt 2Go Reader fügt dem Kontextmenü von Dateien eigene Befehle hinzu. Diese werden angezeigt, wenn Sie mit der rechten Maustaste auf eine Datei klicken. Dateien können direkt über das Kontextmenü entschlüsselt werden.

Verwenden von Drag-and-drop

Ziehen Sie einfach die zu verschlüsselnde oder zu entschlüsselnde Datei auf das Programm-Icon von *u.trust LAN Crypt 2Go Reader*.

Einsehen und Bearbeiten von verschlüsselten Dateien

Dateien können ohne manuelles Entschlüsseln auch direkt bearbeitet werden. Hierbei wird die verschlüsselte Datei beim Öffnen automatisch entschlüsselt und nach der Bearbeitung wieder mit dem entsprechenden Passwort verschlüsselt. Voraussetzung hierfür ist, dass der benötigte Schlüssel schon gespeichert worden ist oder auf Anfrage richtig eingegeben wird.

Zum Bearbeiten der Datei wird das jeweilige Standardprogramm genutzt (ursprüngliche .docx Dateien werden z.B. standardgemäß mit Microsoft Office geöffnet).

Hinweis

- Wenn eine verschlüsselte Datei schreibgeschützt ist, ist auch die temporär entschlüsselte Datei schreibgeschützt. Dies führt in der Regel dazu, dass das jeweilige Standardprogramm Änderungen an der Datei verhindert.
- Um eine entschlüsselte Version einer .pcrypt-Datei zu erstellen, können Sie entweder **Speichern unter** innerhalb des jeweiligen Bearbeitungsprogramms nutzen oder *u.trust LAN Crypt 2Go* öffnen, eine verschlüsselte Datei auswählen und auf die Schaltfläche **Entschlüsseln** tippen.

Sicherheitslücken melden

Utimaco ist sich bewusst, dass hohe Sicherheit durch Zusammenarbeit entsteht. Wir verpflichten uns, verantwortungsbewusst und konstruktiv mit Kunden, Sicherheitsexperten, Sicherheitsforschern und der breiteren Gemeinschaft zusammenzuarbeiten, um Sicherheitslücken zu identifizieren und zu beheben.

Wir begrüßen und fördern die verantwortungsvolle Meldung von Sicherheitslücken. Jede eingehende Meldung wird mit Sorgfalt und Dringlichkeit behandelt. Wir streben an, den Eingang von Meldungen zeitnah zu bestätigen, während des gesamten Untersuchungsprozesses verantwortungsbewusst zu kommunizieren und relevante Aktualisierungen (Sicherheitshinweise und Patches) bereitzustellen, sobald diese verfügbar sind.

Wenn Sie eine Sicherheitslücke entdecken, bitten wir Sie, diese unverzüglich und auf sicherem Weg dem Utimaco PSIRT (Product Security Incident Response Team) zu melden, das Ihre Meldung mit Dringlichkeit bearbeiten wird.

Jede Meldung einer Sicherheitslücke muss mittels PGP-Verschlüsselung verschlüsselt übermittelt werden, um eine versehentliche Offenlegung kritischer Informationen zu verhindern.

(Schritt 1) Bereiten Sie Ihre Meldung vor

Geben Sie möglichst viele Details an, damit wir das Problem verstehen und reproduzieren können:

```
Kurze Zusammenfassung der Sicherheitslücke Beschreibung der Sicherheitslücke Betroffene Produkte, Versionen und Konfiguration Beschreibung der Produktumgebung Verwendetes Betriebssystem. Schrittweise Anleitung zur Reproduktion Mögliche Grundursache. Proof-of-Concept-Code, Screenshots oder Protokolle (falls verfügbar) Mögliche Auswirkungen und vorgeschlagene Abhilfemaßnahmen (optional) Ihre Kontaktinformationen für Rückfragen und Ihr öffentlicher PGP-Verschlüsselungsschlüssel.
```

Alle Meldungen werden streng vertraulich behandelt, und es werden keine personenbezogenen Daten an Dritte weitergegeben

(Schritt 2) Verschlüsseln Sie Ihre E-Mail mit PGP

Zum Schutz sensibler Informationen müssen Sie Ihre Meldung vor dem Versand mit unserem öffentlichen PGP-Schlüssel des PSIRT verschlüsseln.

1. Importieren Sie unseren öffentlichen PSIRT-Schlüssel (unten bereitgestellt) in Ihr PGP/GPG-Tool.
2. Verschlüsseln Sie die Meldung der Sicherheitslücke mit diesem Schlüssel
3. Senden Sie eine E-Mail mit verschlüsseltem Anhang an PSIRT@utimaco.com.
4. Optional können Sie Ihre Nachricht mit Ihrem eigenen PGP-Schlüssel signieren, damit wir die Authentizität überprüfen können.

PSIRT-Kontakt

PSIRT-Team: PSIRT@Utimaco.com

PGP-Fingerabdruck: 77F3 05F8 11AF 228B 7623 33E5 DA5F 264E A9C1 64CB

PGP-Schlüssel: Herunterladen

Technischer Support

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

Unter support.Utimaco.com erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie beispielsweise Knowledge-Items.

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 Utimaco Software sowie ggf. den genauen Wortlaut von Fehlermeldungen ergänzend mit an.

Rechtlicher Hinweis

Copyright © 2024 - 2026 Utimaco IS GmbH, 2018 - 2024 conpal GmbH, 1996 - 2018 Sophos Limited und Sophos Group. Alle Rechte vorbehalten. conpal®, AccessOn® und AuthomaticOn® sind eingetragene Warenzeichen von conpal GmbH.

Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Copyright-Informationen von Drittanbietern finden Sie in dem 3rd Party Software Dokument in Ihrem Produktverzeichnis.

Zuletzt aktualisiert am 21.09.2026