Was ist u.trust LAN Crypt für Android?

u.trust LAN Crypt für Android ermöglicht es Benutzern, dass sie nunmehr auch mithilfe ihrer mobilen Geräte wie Smartphones oder Tablets mit ihren verschlüsselten Daten arbeiten können.

u.trust LAN Crypt ermöglicht unter Windows / macOS mit transparenter Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in kleinen, mittleren und großen Organisationen. Zahlreiche Unternehmen und Organisationen der Wirtschaft sowie öffentlichen Verwaltung in Deutschland und weltweit setzen bereits auf *u.trust LAN Crypt*.

Welche Dateien und Speicherorte durch *u.trust LAN Crypt* geschützt werden sollen und welche Benutzer auf welche Daten zugreifen dürfen, legt ein Security Officer (SO) zentral durch eine oder mehrere Verschlüsselungsrichtlinien fest. Um beispielsweise die Verschlüsselung aller Word-Dokumente in einem zuvor festgelegten Pfad sicherzustellen, definiert der Security Officer die Regel "// Servername/Files/.docx". Sobald diese Regel über eine Richtliniendatei (Policy) auf die Clientrechner mithilfe der *u.trust LAN Crypt* Administration ausgerollt ist, werden fortan sämtliche Word-Dokumente in dieser Freigabe verschlüsselt. Sie können zudem auch mehrere Verschlüsselungsrichtlinien zu einem Verschlüsselungsprofil kombinieren.

Dies gilt grundsätzlich für alle Dateien, unabhängig davon, wo sie gespeichert sind. Sie können damit auf verschlüsselte *u.trust LAN Crypt*-Dateien zugreifen, die entweder lokal, d. h. auf dem Gerät selbst, in einem Netzwerk-Speicher oder auf einem entfernten Speicher, zum Beispiel in einer Cloud, abgelegt sind. Ein Benutzer erhält so auf einfache Weise Zugriff auf die gleichen *u.trust LAN Crypt*-Dateien, die ihm auch an seinem Arbeitsplatz-Rechner zur Verfügung stehen. Diese Version von *u.trust LAN Crypt für Android* ermöglicht zum einen das Bearbeiten und Speichern von verschlüsselten Dateien sowie auf diese per se zuzugreifen und zum anderen die Erweiterung der gewohnten *u.trust LAN Crypt* typischen Sicherheitsinfrastruktur, der Nutzung von Zertifikaten (.p12-Dateien) und der Richtliniendateien (.xml.bz2) für mobile Geräte. Darüber hinaus können Sie mit dieser Version jetzt auch Dateien mit einem sehr sicheren Passwort ver- und entschlüsseln (integriertes u.trust LAN Crypt 2Go).

u.trust LAN Crypt 2Go

Mithilfe des neu integrierten u.trust LAN Crypt 2Go können Sie darüber hinaus Dateien auch passwortbasiert ver- und entschlüsseln. So können Sie auf einfache und sichere Weise Informationen mit anderen Personen austauschen, wie beispielsweise mit Ihren Geschäftspartnern oder auch mit externen Mitarbeitern.

SafeGuard Enterprise: Migration der Dateiverschlüsselung

SafeGuard Enterprise ist eine Sicherheitssuite von Sophos, die aus mehreren Modulen besteht. Data Exchange (DX), Cloud Storage (CS) und File Encryption (FE) bieten alle Verschlüsselung auf Dateiebene. Die gesamte Software-Suite wird jedoch eingestellt, so dass Benutzer Gefahr laufen, den Zugriff auf ihre verschlüsselten Dokumente zu verlieren. Die Umstellung von einem Sicherheitsprodukt auf ein anderes kann mühsam und risikoreich sein, vor allem, wenn die Daten dabei entschlüsselt werden müssen. Bei der Migration zu u.trust LAN Crypt ist dies jedoch nicht der Fall.

u.trust LAN Crypt und Sophos SafeGuard Enterprise sind vollständig kompatibel. Sie verfügen über dieselbe technische Grundlage und dasselbe Subsystem zur Dateiverschlüsselung. Folglich sind die in SafeGuard Enterprise verschlüsselten Dateien vollständig kompatibel mit u.trust LAN Crypt und können von diesem gelesen werden. Die Verschlüsselungsschlüssel sind spezifisch für jede Installation, und nur diese müssen migriert werden.

Schritt 1: Schlüssel aus SafeGuard Enterprise exportieren

Die zum Verschlüsseln von Dateien verwendeten Schlüssel sind für jede SafeGuard Enterprise-Installation eindeutig. Sophos stellt ein einfaches Tool zur Verfügung, mit dem Sie alle in SafeGuard Enterprise zur Verschlüsselung von Dateien verwendeten Verschlüsselungsschlüssel einfach exportieren können. Alle Schlüssel werden bequem in ein einziges Paket kopiert.

Schritt 2: Importieren von Schlüsseln in u.trust LAN Crypt

Die Schlüssel, die jetzt in einem separaten Paket verfügbar sind, können einfach in ein bestehendes u.trust LAN Crypt-System importiert werden. Nach dem Import verfügt die u.trust LAN Crypt-Installation über alles, was sie für den Zugriff auf Dateien benötigt, die mit SafeGuard Enterprise verschlüsselt wurden.

Schritt 3: Richtlinie aktualisieren / Schlüssel zuweisen

Weisen Sie die neu importierten Schlüssel allen Benutzern zu, die Zugriff auf von SafeGuard Enterprise verschlüsselte Dateien benötigen. Diese Schlüssel ermöglichen es den Benutzern, Dateien zu lesen, die in der Vergangenheit mit einem beliebigen SafeGuard Dateiverschlüsselungsmodul verschlüsselt wurden. Dies gilt auch für Dateien, die nach dem Schlüsselimport durch SafeGuard Enterprise verschlüsselt wurden.

Schritt 4: Zugriff auf SafeGuard Enterprise-Dateien

Der u.trust LAN Crypt Client teilt seine technische Grundlage mit SafeGuard Enterprise. Sobald die Schlüssel auf den Client übertragen wurden, kann er alle Dateien lesen, die mit einem der SafeGuard Enterprise-Dateiverschlüsselungsmodule - DX, CS, FS - verschlüsselt wurden. Es besteht keine Notwendigkeit, eine einzelne Datei zu entschlüsseln. Unabhängig davon, wie lange eine Datei verschlüsselt wurde, kann u.trust LAN Crypt sie lesen.

Die vollständige Kompatibilität auf Dateiebene ermöglicht eine reibungslose Migration. Selbst wenn Teile des Unternehmens noch SafeGuard Enterprise verwenden, können alle verschlüsselten Dateien, die sie erstellen, von jedem gelesen werden, der bereits zu u.trust LAN Crypt migriert ist.

Hinweis

- Wenn Sie *SafeGuard Enterprise* installiert haben und eine Migration auf *u.trust LAN Crypt* planen, wenden Sie sich bitte an den u.trust LAN Crypt Support. Weitere Informationen finden Sie unter https://utimaco.com/file-encryption-migration-five-easy-steps-safeguard-enterprise.

Welche Versionen von Android werden unterstützt?

u.trust LAN Crypt für Android unterstützt Android ab Version 9.

u.trust LAN Crypt für Android ist in den Sprachen Deutsch und Englisch verfügbar.

Unterstützte Verschlüsselungs-Algorithmen

Unterstützte Verschlüsselungsalgorithmen für Dateiverschlüsselung

u.trust LAN Crypt für Android unterstützt folgende Verschlüsselungsalgorithmen:

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

Unterstützte Verschlüsselungsalgorithmen für das Key-Wrapping

u.trust LAN Crypt für Android unterstützt folgende Verschlüsselungsalgorithmen für das Key-Wrapping:

- AES-256
- AES-192
- AES-128
- Unterstützt, aber nicht empfohlen: 3DES, 3DES TWO KEY

Durch Key-Wrapping (Standardeinstellung) wird der Transportschlüssel der Security Officer-Daten und der Benutzerprofildaten mit einem per Zufallsverfahren erzeugten Session-Key mit dem ausgewählten Algorithmus verschlüsselt. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel aus dem Zertifikat RSA-verschlüsselt.

Hinweis

- Bitte beachten Sie, dass im Vergleich zu u.trust LAN Crypt für Windows der Algorithmus "RC2" von *u.trust LAN Crypt für Android* nicht unterstützt wird. Wenn das Key-Wrapping für Ihre Richtliniendatei auf den Algorithmus "RC2" eingestellt ist, kann die Richtliniendatei mit *u.trust LAN Crypt für Android* nicht genutzt werden! In dem Fall müssen Sie das Key-Wrapping ändern und hierfür einen der anderen Algorithmen (wie z. B. AES-128) wählen, die unterstützt werden.

Allgemeine Vorbereitungen und Konfiguration

Bitte aktivieren Sie aus Sicherheitsgründen vor der Verwendung dieser App immer die Display-Sperre Ihres Android-Gerätes. Ohne aktivierte Display-Sperre können Sie *u.trust LAN Crypt für Android* nicht ausführen. Verwenden Sie bei der Display-Sperre niemals ein leicht zu erratendes Passwort, wie z. B. "1234" oder "passwort". Nur dann stellen Sie sicher, dass unautorisierte Personen nicht an Ihre vertraulichen Daten gelangen können, wenn z. B. Ihr Android-Gerät einmal verloren gehen oder es Ihnen gestohlen werden sollte. Grundsätzlich empfiehlt Utimaco bei längerer Nichtnutzung des Gerätes oder wenn Sie es gegen ein neues Gerät tauschen, alle vorhandenen App-Daten von *u.trust LAN Crypt* auf dem Android-Gerät zu löschen (siehe App-Daten löschen).

Hinweis

- Wenn Sie die Display-Sperre später deaktivieren, löscht *u.trust LAN Crypt für Android* das Zertifikat und den persönlichen Schlüssel aus dem Zertifikatsspeicher des Android-Gerätes.
- Gerootete Geräte werden von *u.trust LAN Crypt für Android* nicht unterstützt.

Bereitstellen der Konfigurationsdaten

Tippen Sie auf das Zahnradsymbol am unteren Rand der App, um die Einstellungen zu **ÖFFNEN**. Hier können Sie die Konfigurationsdaten angeben:

- Importieren Sie Ihre Richtliniendatei
- Importieren Sie Ihr Benutzerzertifikat

Hinweis

- Insofern die Verteilung Ihrer Konfigurationsdateien über SMB-Freigaben erfolgen soll, wird in den Einstellungen ein zusätzlicher Abschnitt Netzwerk angezeigt. Beachten Sie: Wenn Sie dort die SMB-Zugangsdaten löschen, werden in der Folge auch die Konfigurationsdateien gelöscht.

Verwaltung von Schlüsseln

Sowohl verwaltete Schlüssel als auch passwortbasierte Schlüssel sind in den Einstellungen zu finden. Verwaltete Schlüssel stammen ausschließlich aus der jeweiligen Richtliniendatei, während passwortbasierte Schlüssel in den zugehörigen Einstellungen frei erstellt, umbenannt und gelöscht werden können. Das Umbenennen eines Schlüssels ändert nicht den generierten Schlüssel, der für die Verschlüsselung verwendet wird.

Hinweis

- Passwortbasierte Schlüssel können auch im Rahmen der Verschlüsselung einer Datei erstellt werden. Diese Schlüssel werden dann automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt.
- Durch die erfolgreiche Entschlüsselung durch einen passwortbasierten Schlüssel wird der verwendete Schlüssel automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt.
- Für die Generierung passwortbasierter Schlüssel genutzte Passwörter sind ebenfalls noch nach der Erstellung einsehbar.

Richtlinien

Was sind *u.trust LAN Crypt* Richtliniendateien?

Ein Security Officer (SO) legt über die Administration von *u.trust LAN Crypt* zentral fest, welche Dateien und Speicherorte durch *u.trust LAN Crypt* durch Verschlüsselung geschützt werden sollen und auch, welche Benutzer jeweils auf welche dieser Daten Zugriff erhalten. Hierzu erstellt der Security Officer eine oder mehrere Verschlüsselungsregeln für den Benutzer. Jede einzelne Verschlüsselungsregel besteht aus einem Verschlüsselungspfad und einem Schlüssel sowie einem Verschlüsselungsalgorithmus. Die *u.trust LAN Crypt* Richtliniendateien beinhalten sämtliche Verschlüsselungsregeln, die der Benutzer benötigt, um mit verschlüsselten Dateien arbeiten zu können. Damit der Benutzer die Richtliniendatei verwenden kann, benötigt er zudem ein Zertifikat, das ihm durch den *u.trust LAN Crypt* Security Officer als Schlüsseldatei (.p12-Datei) zur Verfügung gestellt wird. Die Schlüsseldatei enthält das Zertifikat sowie den persönlichen Schlüssel des Benutzers. Der Zugriff auf diese Datei ist passwortgeschützt. Das dazugehörige Passwort erhält der Benutzer durch den Security Officer.

Automatisierter Import mit LAN Crypt Cloud

Wenn der Security Officer (SO) die Administration über die LAN Crypt Cloud durchführt, werden Richtliniendateien und Benutzerzertifikate automatisch geladen. Dafür muss der Nutzer lediglich im Client mit dem entsprechenden LAN Crypt-Konto angemeldet sein. Die Anmeldefunktion kann über das Antippen des Profil-Icons oben rechts in der Anwendung erreicht werden.

Manueller Import von Richtliniendateien

ÖFFNEN Sie die App *u.trust LAN Crypt für Android* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Zahnradsymbol** in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Tippen Sie dort auf die Auswahl **Importieren Sie Ihre Richtliniendatei** und wählen Sie hierüber dann den Speicherort, auf dem sich die Richtliniendatei befindet. Tippen Sie anschließend auf die Richtliniendatei, um sie in die Applikation zu importieren.

Manueller Import von Benutzer-Zertifikaten

ÖFFNEN Sie die App *u.trust LAN Crypt für Android* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Zahnradsymbol** in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Tippen Sie dort auf die Auswahl **Importieren Sie Ihr Zertifikat** und wählen Sie dann den Speicherort, auf dem sich die Schlüsseldatei (.p12-Datei) befindet. Geben Sie dann in dem folgenden Dialog das Passwort ein, das Sie vom Security Officer für Ihr Zertifikat / Ihre Schlüsseldatei erhalten haben. Nachdem Sie das korrekte Passwort eingegeben haben, werden das Zertifikat und der zugehörige private Schlüssel im Zertifikatsspeicher der Applikation gespeichert.

Hinweis

- *u.trust LAN Crypt für Android* unterstützt auch die Angabe von mehreren Zertifikaten des Benutzers in der Richtliniendatei. Um die Richtliniendatei verwenden zu können, muss der Benutzer mindestens im Besitz von einem seiner Zertifikate sein, die ihm ausgestellt wurden und mit dessen öffentlichen Schlüssel die Richtliniendatei verschlüsselt ist, bzw. muss er dieses auch importiert haben.

Zertifikatsinformationen

ÖFFNEN Sie die App *u.trust LAN Crypt für Android* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Zahnradsymbol** in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Tippen Sie dort auf die Auswahl **Zertifikatsinformationen**. Sie erhalten im nächsten Dialog eine Übersicht der auf dem Gerät installierten Zertifikate. Tippen Sie auf das gewünschte Zertifikat, von dem Sie weitere Informationen erhalten wollen. Danach werden Ihnen die weiteren Details, wie z. B. die Serien-Nummer, der Gültigkeitszeitraum etc., des Zertifikats angezeigt. Sie können sich diese Informationen auch in die Zwischenablage kopieren, wenn Sie weiter unten im Teildialog auf **Kopiere in Zwischenablage** tippen. Durch Tippen auf **OK** schließen Sie den Dialog.

Richtliniendateien und Zertifikate mithilfe von MDM ausrollen

Die Konfigurationsdaten bestehen aus einer Liste, die Schlüssel und Zeichenfolgen beinhaltet. Die Dateien müssen als Base64-kodierte Zeichenkette über eine URL bereitgestellt werden, die auf einem HTTPS oder SMB-Server gehostet wird. Die folgenden Konfigurationsschlüssel werden von *u.trust LAN Crypt* angeboten.

Hinweis

- Wird *u.trust LAN Crypt für Android* über MDM ausgerollt, kann neben der Richtliniendatei und dem Benutzerzertifikat auch das öffentliche Zertifikat (.cer) des Sicherheitsbeauftragten, mit welchem die Richtliniendatei signiert wurde, auf dem mobilen Gerät bereitgestellt werden. In diesem Fall werden auch vom Benutzer manuell importierte Policy-Dateien durch Validierung der Signatur des Security-Officer-Zertifikats geprüft.

Einstellungen

Die Konfigurationsdaten sind eine Liste von Key+String-Tupeln. Die Dateien müssen als Base64-kodierte Strings über eine URL bereitgestellt werden, die auf einem HTTPS- oder SMB-Server gehostet wird. Die folgenden Konfigurationsschlüssel werden von *u.trust LAN Crypt* angeboten:

Betriebsmodus

operation_mode: Kann verwendet werden, um die Konfigurationsoptionen der App einzuschränken **(STRING)**.

- Mögliche Werte:
  - `"cloud"`: Nur die LAN-Crypt Cloud Administration kann verwendet werden.
  - `"classic"`: Nur die LAN Crypt On-Premise Administration (Nutzung von Richtliniendateien) kann verwendet werden.
  - Kein Wert: Cloud- oder On-Premise Administration sind möglich.

Hinweis

- Wenn *operation_mode* nicht gesetzt ist oder einen ungültigen Wert hat und eine der MDM-Einstellungen gesetzt ist (*policy_url*, *policy_blob*, *usercert_url*, *usercert_blob*, *admcert_url*, *admcert_blob*), wird `"classic"` von der App erzwungen.

Schlüssel für die Richtliniendatei

policy_blob: Richtliniendatei im Format XML oder XML.bz2 (komprimiert) als Base64-kodierte Zeichenfolge **(STRING)**.

policy_url: URL zu einer Richtliniendatei im Format XML oder XML.bz2 **(STRING)**.

Schlüssel für das Benutzerzertifikat / P12-Datei

usercert_blob: PKCS-12-Zertifikatsdatei als Base64-kodierte Zeichenfolge **(STRING)**.

usercert_url: URL zu einer PKCS-12-Zertifikatsdatei **(STRING)**.

Schlüssel für Security Officer-Zertifikate

admcert_blob: Security Officer-Zertificat ("cer"-Datei / DER-kodiert) als Base64-kodierte Zeichenfolge **(STRING)**.

admcert_url: URL zu einem Security Officer-Zertifikat ("cer"-Datei / DER-kodiert) **(STRING)**.

Standardschlüssel

default_key_guid: GUID des Standardschlüssels, der für die Verschlüsselung neuer Dateien verwendet werden muss **(STRING)**.

Hinweis

- Ist ein Standardschlüssel gesetzt, so kann der Benutzer ausschließlich diesen Schlüssel zur Verschlüsslung nutzen. Die Verschlüsselung durch einen

passwortbasierten Schlüssel ist jedoch trotzdem jederzeit möglich. Diese führt dann zu einer verschlüsselten Kopie der Originaldatei.

Schlüssel für Samba-Anmeldedaten

smb_username: Verweist eine der Einstellungen für die Richtliniendatei oder für das Zertifikat auf einen SMB-Speicherort kann hier der Benutzername für die SMB-Verbindung über diesen Schlüssel konfiguriert werden **(STRING)**.

Hinweis

- Wird kein Wert für diesen Schlüssel definiert, wird der Benutzer aufgefordert neben seinem Passwort auch seinen Benutzernamen für die SMB-Verbindung einzugeben. Aus Sicherheitsgründen muss die Eingabe des Passwortes für die SMB-Verbindung immer durch den Benutzer erfolgen.

Schlüssel für Zertifikatsüberprüfung

cert_validation: Aktiviert die Zertifikatsüberprüfung **(BOOLEAN)**.

Hinweis

- Eine Zertifikatsüberprüfung erfolgt nicht, wenn diese Einstellung fehlt.

Kompatibilität

microsoft_office_support: Erlaubt das Editieren von Dateien mit Microsoft Office Anwendungen **(BOOLEAN)**.

Hinweis

- Die Office-Unterstützung ist deaktiviert, wenn die Einstellung fehlt. Die Einstellung erfordert außerdem, dass die Berechtigung "Verwaltung aller Dateien zulassen" auch in der Microsoft Office App aktiviert ist.

Richtlinien-Gültigkeitsdauer

cache_timeout_hours: Anzahl der Stunden, die eine Richtlinie gültig bleibt, ohne eine Verbindung zum Server herzustellen **(INTEGER)**.

Hinweis

- Diese Einstellung ist nur relevant, wenn ein SMB-Freigabe verwendet wird, um Richtlinien oder Zertifikate zu importieren

Samsung eSE

enable_samsung_ese: Aktiviert die Nutzung von Samsung eSE. **(BOOLEAN)**.

Regeln

- Vordefinierte Einstellungen können durch den Benutzer nicht geändert oder außer Kraft gesetzt werden.
- URLs müssen auf HTTPS-Servern mit einem gültigen SSL-Zertifikat gehostet werden. Sie können dies überprüfen, indem Sie die URL in einem Browser (z. B. Chrome, Safari) auf dem mobilen Gerät eingeben. Wenn die Datei angezeigt werden kann, wird auch die URL als Konfigurationswert funktionieren.
- Wenn sowohl BLOB als auch URL für eine Einstellung unterstützt werden, hat der BLOB Vorrang.
- Wenn der Daten-BLOB oder die URL einer Einstellung ungültig ist, wird eine Fehlermeldung angezeigt.
- Bei der Verwendung von URLs für SMB-Freigaben werden Benutzernamen und Passwörter ignoriert (verwenden Sie stattdessen smb_username)(smb://localfileserver/certificates/sepp.p12)
- Format der Eingabe: smb://<Host>/<Freigabe>/<Ordner>/<Dateiname>
- Es bestehen zwar grundsätzlich keine Einschränkungen bezüglich der Länge von Zeichenfolgen, die Konfigurationsdatei sollte aber dennoch nicht größer als ein paar Kilobyte sein.

App-Daten löschen

u.trust LAN Crypt für Android zurücksetzen

Wählen Sie in den App-Einstellungen von *u.trust LAN Crypt für Android* die Option App-Daten löschen. Damit löschen Sie alle in der *u.trust LAN Crypt*-App gespeicherten Daten, einschließlich der Richtliniendatei, des Benutzerzertifikates und des privaten Schlüssels. *u.trust LAN Crypt für Android* befindet sich danach wieder im Auslieferungszustand.

Dateien öffnen, bearbeiten, verschlüsseln, entschlüsseln und freigeben

Mit *u.trust LAN Crypt für Android* wird der Zugriff auf Dateien ermöglicht, die auf dem Gerät selbst gespeichert sind (lokaler Speicher und auch Daten, die sich auf der eingesteckten SD-Speicherkarte befinden), die sich auf Netzwerkfreigaben oder die sich auf entfernten Speichersystemen (z. B. auf OneDrive oder Google Drive) befinden. Der Dateizugriff über *u.trust LAN Crypt für Android* kann direkt oder aber auch über das "Storage Access Framework (SAF)" erfolgen. SAF ermöglicht den Remote-Zugriff zu nutzen, der von anderen auf demselben Gerät installierten Apps bereitgestellt wird. So kann beispielsweise die *u.trust LAN Crypt*-App auf die Daten des Benutzers in OneDrive zugreifen, wenn die OneDrive-App installiert ist. In ähnlicher Weise erfolgt dann auch der Zugriff auf Google Drive, wenn die zugehörige App auf dem mobilen Gerät installiert ist etc.

Hinweis

- Möglicherweise müssen Sie sich zuerst bei Ihrem OneDrive- oder Google Drive-Konto anmelden, um dort auf Dateien zugreifen zu können. Dies gilt auch für den Zugriff auf Dateien über eine Windows-Freigabe (SMB).

Wie erfolgt der Zugriff auf verschlüsselte Dateien?

Auf Dateien eines mobilen Gerätes kann wie zuvor schon zum Teil beschrieben auf verschiedene Weise zugegriffen werden. Dies kann über eine native Dateibrowser-App, eine proprietäre App für Cloud-Speicher (wie z. B. OneDrive) oder auch direkt aus einer Anwendungs-App heraus erfolgen. *u.trust LAN Crypt für Android* enthält auch einen eigenen integrierten Dateibrowser. Über das Dashboard kann somit auch direkt auf (verschlüsselte) Dateien zugegriffen werden, die sich entweder auf einem lokalen Speicherort, in einer Windows-Freigabe (SMB) oder im Cloud-Speicher von z. B. OneDrive befinden. Über den internen Dateibrowser können Sie sich aber auch die Verschlüsselungsinformationen der dort vorhandenen Dateien anzeigen lassen. Ist eine Datei mit einem grünen Schlüsselsymbol markiert, bedeutet dies, dass die Datei verschlüsselt ist und Sie den erforderlichen Schlüssel besitzen, um diese Datei lesen und bearbeiten zu können. Ein rotes Schlüsselsymbol dagegen bedeutet, dass die Datei zwar von *u.trust LAN Crypt* verschlüsselt ist, Sie aber nicht in Besitz des erforderlichen Schlüssels sind, um diese Datei lesen oder bearbeiten zu können.

Dateien öffnen, bearbeiten und verschlüsselt speichern

Um Dateien zu bearbeiten, lassen sich diese auch direkt aus der Anwendungs-App über den integrierten Dateibrowser über das jeweilige Kontextmenü laden. Die Dateien können Sie dann bearbeiten. Beim Speichern werden sie dann automatisch von *u.trust LAN Crypt für Android* verschlüsselt.

Hinweis

- Für die Bearbeitung von Office-Dokumenten empfiehlt Utimaco die quelloffene und kostenlose App "Collabora Office" zu nutzen. Diese basiert auf LibreOffice, die zu den bekanntesten und beliebtesten quelloffenen Office-Anwendungen weltweit gehören.

Benutzer können somit ihre Dateien mit einem nativen Dateibrowser, über den integrierten Dateibrowser, direkt aus einer Anwendungs-App sowie über die App *u.trust LAN Crypt für Android* durchsuchen, **ÖFFNEN**, bearbeiten und speichern. Um eine verschlüsselte Datei über den integrierten Dateibrowser zu **ÖFFNEN**, tippen Sie auf das **Ordnersymbol** links unten innerhalb der App. Wählen Sie dann über das Menü (OneDrive, Windows Freigabe (SMB) oder Durchsuchen) den Speicherort, auf dem sich die Datei befindet.

Über den Dateibrowser wählen Sie dann den Pfad und dort die verschlüsselte Datei, die Sie über die *u.trust LAN Crypt*-App **ÖFFNEN** wollen. Tippen Sie auf diese Datei und tippen Sie danach im erweiterten Menü auf die Auswahl **ÖFFNEN**. Es öffnet sich der Dialog Teilen. Wählen Sie dort dann die Anwendungs-App aus, mit der Sie diese Datei **ÖFFNEN** bzw. bearbeiten wollen (z. B. Collabora Office). Danach wird die zuvor ausgewählte Datei über die Anwendungs-App auf Ihrem Mobilgerät geöffnet und entschlüsselt angezeigt. Sie können diese dann bearbeiten und auch wieder speichern. Die Verschlüsselung der Datei erfolgt bei diesem Vorgang automatisch.

Hinweis

- Auf dem Speicherort selbst bleibt diese Datei stets verschlüsselt. Alle Ver- und Entschlüsselungsvorgänge von *u.trust LAN Crypt für Android* erfolgen nur innerhalb

des geschützen Datenbereiches der App auf dem mobilen Android-Gerät. Zugriff auf diesen Datenbereich hat ausschließlich *u.trust LAN Crypt für Android*.

Verschlüsselungsinformationen anzeigen lassen

Über ein Symbol in der rechten oberen Ecke der Miniaturansicht wird der jeweilige Status der Datei angezeigt:

- **grüner Schlüssel:** Die Datei ist verschlüsselt und sie kann von Ihnen geöffnet werden.
- **grauer Schlüssel:** Die Datei ist unverschlüsselt und sie kann von Ihnen geöffnet werden.
- **roter Schlüssel:** Die Datei ist verschlüsselt und kann nicht geöffnet werden (der Schlüssel ist entweder nicht verfügbar oder der verwendete Verschlüsselungsalgorithmus wird für mobile Geräte nicht unterstützt).

Um weitere Informationen zu erhalten, drücken Sie etwas länger auf eine Datei. Es öffnet sich ein Kontextmenü, über welches Sie nun die Auswahl **Verschlüsselungsinfos** treffen können. Im Abschnitt **Verschlüsselungsinfos** werden nun detaillierte Informationen angezeigt:

- **Verschlüsselungsstatus:** Zeigt an, ob die Datei verschlüsselt ist oder nicht.
- **Schlüsselname:** Zeigt den Namen des Schlüssels an, mit dem die Datei verschlüsselt ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Schlüssel-ID:** Zeigt die GUID des Schlüssels an, mit dem die Datei verschlüsselt ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Schlüssel verfügbar:** Zeigt an, ob der Schlüssel in der Richtliniendatei vorhanden ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Auf Mobilgeräten unterstützt:** Zeigt an, ob der verwendete Verschlüsselungsalgorithmus vom mobilen Gerät unterstützt wird (wird nur bei verschlüsselten Dateien angezeigt, bei welchem das Verschlüsselungsverfahren nicht unterstützt wird).

Datei mit einem Schlüssel aus der Richtliniendatei verschlüsseln

Um eine Datei mit einem Schlüssel aus der Richtliniendatei zu verschlüsseln, **ÖFFNEN** Sie die App *u.trust LAN Crypt für Android* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Ordnersymbol** in der unteren linken Ecke, um die Dateimenüansicht zu **ÖFFNEN**. Wählen Sie dort den gewünschten Speicherort (OneDrive, Windows Freigabe (SMB) oder Durchsuchen) aus, der die Datei enthält, die Sie verschlüsseln möchten. Wählen Sie dann die Datei aus, die Sie verschlüsseln möchten. Tippen Sie anschließend im erweiterten Menü auf die Auswahl **Verschlüsseln**. Wählen Sie die Option zur Verschlüsselung mit einem gespeicherten Schlüssel.

Aktivieren Sie die Option **Vorhandene Datei überschreiben**, falls die Originaldatei verschlüsselt werden soll, und tippen Sie auf **OK**. Die Datei wird dann verschlüsselt an dem zuvor ausgewählten Ort gespeichert. Wenn Sie die Originaldatei nicht überschreiben möchten, deaktivieren Sie die Option **Vorhandene Datei überschreiben** und tippen Sie auf **OK**. Das Dialogfeld Freigeben wird geöffnet. Wählen Sie aus der dort angezeigten Liste der Apps die jeweilige App aus, mit der Sie die verschlüsselte Datei speichern oder ggf. teilen möchten (z.B. Google Drive, Gmail etc.) und tippen Sie auf diese. Die Datei wird dann verschlüsselt an diese App übertragen. Mit der Option **In der Nähe** können Sie die verschlüsselte Datei auch über Wi-Fi oder Bluetooth mit einem Gerät in der Nähe teilen.

Hinweis

- Wenn kein Standardverschlüsselungsschlüssel für Sie eingerichtet wurde, können Sie den Verschlüsselungsschlüssel in der Liste ändern, indem Sie auf einen anderen verfügbaren Schlüssel tippen. In diesem Fall wird die Datei mit diesem Schlüssel anstelle des zuvor ausgewählten Schlüssels verschlüsselt.

Datei mit einem Passwort verschlüsseln und teilen (u.trust LAN Crypt 2Go)

Um eine Datei mit einem passwortbasierten Schlüssel zu verschlüsseln und freizugeben, **ÖFFNEN** Sie die *u.trust LAN Crypt für Android*-App auf Ihrem Mobilgerät. Tippen Sie dann auf das **Ordnersymbol** in der unteren linken Ecke der App, um die Dateimenüansicht zu **ÖFFNEN**. Wählen Sie dort den Speicherort (OneDrive, Windows Freigabe (SMB) oder Durchsuchen) aus, der die Datei enthält, die Sie verschlüsseln oder vielleicht freigeben möchten. Wählen Sie dann die Datei aus, die Sie verschlüsseln möchten, indem Sie auf sie tippen. Tippen Sie anschließend im erweiterten Menü auf die Auswahl **Verschlüsseln**. Wählen Sie die Option zur **Verschlüsselung mit einem passwortbasierten Schlüssel**. Nun können Sie entweder ein bereits verwendetes Passwort auswählen oder ein neues Passwort für die Verschlüsselung erstellen. Wenn Sie auf diese Weise ein neues Kennwort erstellen, wird das Kennwort automatisch auf dem Gerät gespeichert und kann zum weiteren Ver- und Entschlüsseln von Dateien verwendet werden. Passwortbasierte Schlüssel können auch im

Einstellungsmenü gefunden und bearbeitet werden. Der **Freigabe-Dialog** öffnet sich. Wählen Sie aus der dort angezeigten Liste der Apps die jeweilige App aus, mit der Sie die verschlüsselte Datei speichern oder ggf. teilen möchten (z.B. Google Drive, Gmail, etc.) und tippen Sie darauf. Die Datei wird dann verschlüsselt an diese App übertragen und kann je nach Funktionalität (z.B. nativer Dateibrowser oder Google Drive, etc.) bearbeitet, gespeichert oder mit anderen (z.B. Gmail) geteilt werden. Mit der Option **In der Nähe** können Sie die verschlüsselte Datei auch mit einem Gerät in der Nähe über Wi-Fi oder Bluetooth teilen.

Hinweis

- Die Verschlüsselung erfordert immer ein sicheres Passwort! Dieses muss aus mindestens 8 Zeichen bestehen sowie Groß- und Kleinschreibung, Ziffern und Sonderzeichen beinhalten. Das für den Schlüssel genutzte Passwort kann im Nachhinein noch in den Einstellungen eingesehen werden.
- Der Name des Verschlüsselungspassworts hat keinen Einfluss auf den für die Verschlüsselung verwendeten Schlüssel. Der eigentliche Schlüsselwert für die Verschlüsselung wird separat erzeugt.
- Anders als bei der Verschlüsselung an Ort und Stelle mit einem Schlüssel aus der Richtliniendatei wird bei der Verschlüsselung mit einem kennwortbasierten Schlüssel die Originaldatei nicht manipuliert, sondern eine verschlüsselte Kopie der Datei erstellt, die dann geteilt oder abgespeichert werden kann.

Datei entschlüsseln und teilen

Um eine Datei zu entschlüsseln, **ÖFFNEN** Sie die *u.trust LAN Crypt für Android*-App auf Ihrem mobilen Gerät. Tippen Sie dann auf das **Ordnersymbol** unten links in der App, um die Dateimenüansicht zu **ÖFFNEN**. Wählen Sie dort den Speicherort (OneDrive, Windows Freigabe (SMB) oder Durchsuchen) aus, an dem die Datei, die Sie entschlüsseln oder vielleicht freigeben möchten, gespeichert ist. Wählen Sie dann die Datei aus, die Sie entschlüsseln möchten, indem Sie auf sie tippen. Tippen Sie anschließend im erweiterten Menü auf die Auswahl **ENTSCHLÜSSELN**. Handelt es sich bei der Datei um eine passwortgeschützte Datei, wird an dieser Stelle möglicherweise ein zusätzlicher Dialog angezeigt. Geben Sie in diesem Fall das erforderliche Kennwort in das Feld Kennwort eingeben ein. Der **Freigabe-Dialog** öffnet sich. Wählen Sie aus der dort angezeigten Liste der Apps die jeweilige App aus, mit der Sie die verschlüsselte Datei speichern oder ggf. teilen möchten (z.B. Google Drive, Gmail, etc.) und tippen Sie darauf. Die Datei wird dann verschlüsselt an diese App übertragen und kann je nach Funktionalität (z.B. nativer Dateibrowser oder Google Drive, etc.) bearbeitet, gespeichert oder mit anderen (z.B. Gmail) geteilt werden. Mit der Option **In der Nähe** können Sie die entschlüsselte Datei auch mit einem Gerät in der Nähe über Wi-Fi oder Bluetooth teilen.

Hinweis

- Wenn Sie denselben Speicherort wählen, werden Sie in einem weiteren Dialog gefragt, ob Sie die vorhandene Datei ersetzen möchten.
- Bei erfolgreicher Entschlüsselung einer Datei mit einem passwortbasierten Schlüssel wird der verwendete Schlüssel automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt. Die Liste der passwortbasierten Schlüssel kann in den Einstellungen gefunden und bearbeitet werden. Ebenfalls kann dort das für den passwortbasierten Schlüssel genutzte Passwort eingesehen werden.

Windows Freigabe (SMB)

u.trust LAN Crypt für Android ermöglicht das Hinzufügen mehrerer Windows-Freigaben (SMB), die im Reiter **Dateien** verwaltet werden können. Darüber hinaus bietet die Dateiverwaltung mit LAN Crypt auf den einzelnen Windows-Freigaben erweiterte Funktionen.

Erweiterte Dateiverwaltung auf Windows Freigaben (SMB)

Die Dateiverwaltung auf einer Windows-Freigabe bietet zusätzlich zu den grundlegenden Funktionen von *u.trust LAN Crypt für Android* erweiterte Optionen wie das Kopieren und Verschieben von Dateien sowie das Erstellen, Löschen und Umbenennen von Ordnern und Dateien. Des Weiteren besteht die Möglichkeit, Dateien hochzuladen. Für die Durchführung dieser zusätzlichen Aktionen ist es erforderlich, dass der Nutzer die entsprechenden Verschlüsselungsregeln für die Dateien und Ordner zugewiesen bekommen hat.

Beim Kopieren, Verschieben und Hochladen von Dateien führt das System eine automatische Überprüfung der geltenden Verschlüsselungsrichtlinien durch. Falls erforderlich, wird der Benutzer gefragt, ob die Datei gemäß den neuen Verschlüsselungsanforderungen verschlüsselt werden soll.

Hinweis

- Das Löschen von Ordnern wird nur für leere Ordner unterstützt.

Protokollfunktion

u.trust LAN Crypt für Android verfügt über eine ausführliche Protokollierung. **Diese dient ausschließlich zur Fehleranalyse und sollte daher von Ihnen nur dann aktiviert werden, wenn mit dieser App Fehler oder Probleme auftreten sollten.**

Erweiterte Protokollierung

Die Funktion **Ausführliche Protokollierung** können Sie über die Einstellungen von *u.trust LAN Crypt für Android* jederzeit aktivieren und deaktivieren. Um diese Funktion zu aktivieren, **ÖFFNEN** Sie die App *u.trust LAN Crypt für Android* auf Ihrem Mobilgerät. Tippen Sie dann auf das Zahnradsymbol in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Aktivieren Sie die Protokollfunktion, indem Sie den Schieberegler für die **Ausführliche Protokollierung** nach rechts bewegen. Die Protokollfunktion wird dann als aktiviert (rot) angezeigt. Führen Sie dann alle weiteren Schritte aus, die zu einem Fehler geführt haben.

Hinweis

- Die Logdateien speichern keine sensiblen Informationen ab!

Protokolldateien senden

Mithilfe der Funktion **Protokolldateien senden** können Sie diese Protokollinformationen zu Analysezwecken dann an den Utimaco-Support als E-Mail versenden. Tippen Sie hierfür auf das Symbol **Teilen**, das rechts neben **Protokolldateien senden** angezeigt wird. Wählen Sie dann die App, die Sie für Ihre E-Mail-Kommunikation nutzen. Die Protokolldatei wird der E-Mail dann automatisch als komprimierte Datei (.zip) angehängt. Deaktivieren Sie die Funktion **Erweiterte Protokollierung**, indem Sie erneut auf den Schieberegler tippen. Die Erweiterte Protokollierung wird dann wieder als deaktiviert (grau) angezeigt.

Kompatibilität mit Cloud-Diensten

LAN Crypt unterstützt die Verschlüsselung von Dateien auch auf cloudbasierten Speichermedien und bietet damit einen zusätzlichen Schutz vor unbefugtem Zugriff - selbst durch die Betreiber der jeweiligen Cloud-Dienste. Cloud-Anbieter wie Microsoft, Google oder ähnliche Plattformen stellen üblicherweise zusätzliche Funktionen bereit, beispielsweise die kollaborative Bearbeitung von Dokumenten oder die inhaltsbasierte Suche von Dateien. Da Cloud-Dienste keinen Zugriff auf den Inhalt verschlüsselter Dateien erhalten, stehen diese Funktionen für von LAN Crypt geschützte Dateien nicht zur Verfügung. Die verschlüsselten Daten unterliegen einem besonders hohen Schutz und können daher von den Diensten nicht verarbeitet werden.

Nicht kompatible Microsoft-365-Dienste

Folgende Microsof-365-Funktionen setzen eine inhaltliche Analyse der Dateien voraus und sind daher nicht nutzbar, wenn die Dateien durch LAN Crypt verschlüsselt sind:

- Nachrichtenflussregeln, einschließlich Anti-Schadsoftware- und Spam-Prüfungen, die Zugriff auf Anlagen benötigen
- Microsoft Delve
- eDiscovery
- Inhaltssuche und -indizierung
- Office Web Apps, einschließlich Funktionen zur gemeinsamen Dokumentbearbeitung
- Copilot

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

Technische Unterstützung

Technischen Support zu Utimaco Produkten können Sie wie folgt abrufen:

Unter support.Utimaco.com erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie 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 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