Encryption 2.0: ownCloud's Verschlüsselungs-Modell

Datenschutz ist eine zentrale Anforderung an eine Unternehmenslösung für Filesync und –share und setzt sicheren und zuverlässigen Austausch von Informationen und Dateien voraus. Encryption 2.0 ist ein modular aufgebautes und flexibles Framework, das leistungsfähige Funktionen für die serverseitige Verschlüsselung von Daten bei der Speicherung bereitstellt. ownCloud's offene Architektur ermöglicht außerdem die Integration von Technologien wie OpenSSL, um Daten während der Übertragung zu schützen. Darüber hinaus können komplexe Sicherheitsanforderungen, wie eine clientseitige Verschlüsselung durch einfache Erweiterung unterstützt werden.

Verschlüsselung mit ownCloud Encryption 2.0

Mit der neuen Verschlüsselungs-Applikation profitieren Kunden nun von zusätzlicher Modularität und Flexibilität bei der Gestaltung ihrer Architektur. Sie sind nicht mehr auf die Nutzung des integrierten Verschlüsselungsmodells beschränkt, sondern können flexibel die Lösung wählen, die für ihre Umgebung, ihre Geschäftsprozesse und die Einhaltung von gesetzlichen Auflagen am besten geeignet ist.

Kunden profitieren mit der neuen Version von zwei Vorteilen: Sie können ihre Keys im eigenen Keystore verwalten und zugleich den Verschlüsselungsmechanismus an ihre Bedürfnisse anpassen. ownCloud ist der einzige Anbieter, der diese Möglichkeit bietet. Indem die Verwaltung der Keys vom eigentlichen Verschlüsselungsalgorithmus entkoppelt wird, ermöglicht Encryption 2.0 flexible Anpassungen des Verschlüsselungsverfahrens an geänderte Anforderungen und neue behördliche Auflagen. Außerdem können auch mehrere Verschlüsselungsmodule gleichzeitig unterstützen werden, sodass die IT-Abteilung über die nötige Flexibilität und Kontrolle verfügt.

Das zentrale Verschlüsselungsmodell von ownCloud

Funktionsweise der serverseitigen Verschlüsselungsanwendung (Abbildung 2):

- ownCloud erzeugt für jeden Nutzer automatisch ein 4.096 Bit starkes Schlüsselpaar aus privatem und öffentlichem Key. Die privaten Keys werden nach dem AES-256-Verfahren mit dem Anmeldepasswort des Nutzers verschlüsselt.

  Hinweis: Immer wieder kommt es vor, dass ein Anwender sein Passwort vergisst. ownCloud ermöglicht es Administratoren, eine optionale Recovery-Key-Funktion zu aktivieren, mit der der Zugriff auf Daten wiederhergestellt werden kann, wenn das zugehörige Passwort vergessen wurde. Diese Funktion wird zentral aktiviert. Anschließend kann jeder Anwender selbst entscheiden, ob er sie auch für sein ownCloud-Benutzerkonto aktivieren möchte.

- Beim Hinzufügen oder Synchronisieren von Dateien erzeugt ownCloud einen Key für die entsprechende Datei und verschlüsselt damit die Datei nach dem AES-256-Verfahren. Damit verfügt jede Datei in ownCloud über einen eindeutigen Key.
- Auch dieser Key selbst wird von ownCloud mit dem öffentlichen Key aller Benutzer, die auf die Datei zugreifen können, verschlüsselt. So entstehen bei dieser Verschlüsselung ein oder mehrere gemeinsame Keys. Jeder Anwender verfügt über einen eindeutigen gemeinsamen Key für jede Datei, auf die er zugreifen kann.
- Wenn ein autorisierter Nutzer einen Dateizugriff anfordert, entschlüsselt ownCloud den Key für diese Datei mit einer Kombination aus dem privaten Key des Nutzers und dem zugehörigen gemeinsamen Key. Anschließend wird die physische Datendatei mit dem Datei-Key entschlüsselt.
- Wird eine Datei später für einen weiteren Nutzer freigegeben, wird der Key für die Datei wieder mit dem öffentlichen Key dieses Nutzers verschlüsselt, wodurch ein neuer gemeinsamer Key erzeugt wird. Zwar führt diese Abstraktion dazu, dass ownCloud den Key für die Datei erneut verschlüsseln muss, doch lässt sich damit der wesentlich höhere Aufwand für die erneute Verschlüsselung der gesamten physischen Datei zur Freigabe der Datei für neue Anwender vermeiden.

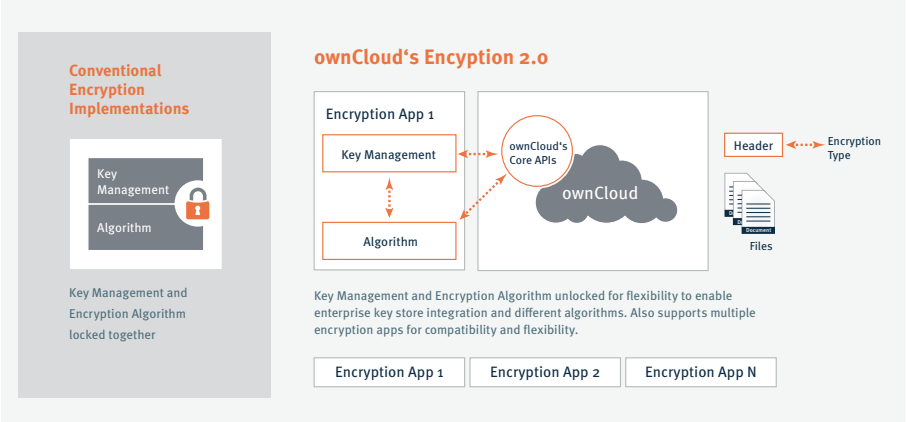

Abbildung 1: Verschlüsselung mit ownCloud Encryption 2.0

Dieser Vorteil kommt auch dann zum Tragen, wenn einem Anwender Zugriffsrechte für eine oder mehrere Dateien entzogen werden sollen.

Vorteile des Verschlüsselungs-Modells von ownCloud

- Das Modell ist hochgradig sicher – es wurde nach bewährten und weitverbreiteten Technologien wie OpenSSL und Standards wie AES-256 implementiert, was empfohlen wird von namhaften Organisationen, wie NIST oder BSI.
- Es bietet auch für Unternehmen mit vielen Anwendern und sehr großen Dateien eine optimierte Performance.
- Dateien können sicher in jedem unterstützten Format auf einer für ownCloud zugänglichen Speicherfreigabe oder auch extern gespeichert werden, ohne dass Dritte Zugriff auf die Daten erhalten.
- Im Gegensatz zu anderen Lösungen für Filesync und -share bietet ownCloud den Administratoren vollständige Kontrolle über die Keys für die Dateiverschlüsselung.
- Dank seiner Offenheit kann das Modell von ownCloud an zukünftige Anforderungen angepasst werden. Um beispielsweise zu einem späteren Zeitpunkt Erweiterungen für eine Ende-zu-Ende Verschlüsselung vorzunehmen, sind keine größeren Anpassungen erforderlich.

Zusammenfassung

Das Verschlüsselungsmodell ownCloud Encryption 2.0 kombiniert beispiellose Flexibilität mit bewährten Technologien für die serverseitige Verschlüsselung von Daten bei der Speicherung und einer Architektur, die durch einfache Erweiterung auch komplexe Sicherheitsanforderungen unterstützen kann. Auf der Grundlage bewährter, weitverbreiteter Technologie unterstützt ownCloud Datenschutzbestimmungen für unterschiedlichste Speicherformate, ohne dabei die Daten Risiken auszusetzen.

Das Verschlüsselungsmodell von ownCloud ist hochgradig skalierbar und bietet Administratoren vollständige Kontrolle über die für die Verschlüsselung verwendeten Keys und Datenflüsse.

Mit Encryption 2.0 von ownCloud können Kunden ihr Verschlüsselungsmodell um eine eigene Lösung für die Verwaltung von Keys ergänzen oder die grundlegenden Funktionen des ownCloud Core für das Speichern von Keys verwenden.

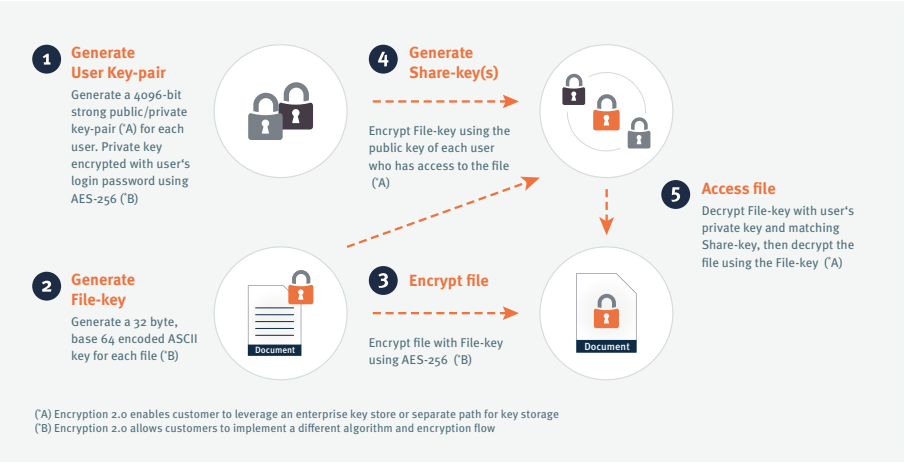

Abbildung 2: ownCloud's Server Side Encryption Functions

Sicher, schnell, skalierbar und flexibel – Mit ownCloud können Unternehmen unterschiedlichste Ziele im Hinblick auf den Austausch von Dateien zuverlässig unterstützen.

Weitere Informationen finden Sie auch in dem Whitepaper „Optimale Sicherheit für Ihre ownCloud-Umgebung“ unter https://owncloud.com/de/whitepapers

Technische Referenzen

1. Erzeugen von Schlüsselpaaren mit privatem/öffentlichem Key für einen Benutzer: http://www.php.net/manual/de/function.openssl-pkey-new.php
2. Erzeugen von base64-Keys zur Verschlüsselung von Dateien: http:/www.php.net/openssl_random_pseudo_bytes
3. Verschlüsseln von Dateien mit dem erzeugten Key http://php.net/manual/de/function.openssl-encrypt.php
4. Verschlüsseln des Datei-Keys mit dem öffentlichen Key aller Anwender mit Zugriffsrechten für die Datei zur Erzeugung des gemeinsamen Keys: http://php.net/manual/de/function.openssl-seal.php
5. Entschlüsseln des Datei-Keys: http://php.net/manual/de/function.openssl-open.php
6. Entschlüsseln der Datei mit dem Datei-Key: http://php.net/manual/de/function.openssl-decrypt.php

ownCloud GmbH
Leipziger Platz 21
90491 Nürnberg
Germany

www.owncloud.com/contact
phone: +49 911 14888690

www.owncloud.com

@ownCloud
facebook.com/owncloud
gplus.is/owncloud
linkedin.com/company/owncloud