Leitfaden

agree21Doksharing – Ende-zu-Ende-Verschlüsselung

Stand: Juli 2022
Version 1.3

ATRUVIA

Genossenschaftliche FinanzGruppe Volksbanken Raiffeisenbanken

agree21Doksharing - Ende-zu-Ende-Verschlüsselung

Inhaltsverzeichnis

1 Allgemeines zur Verschlüsselung

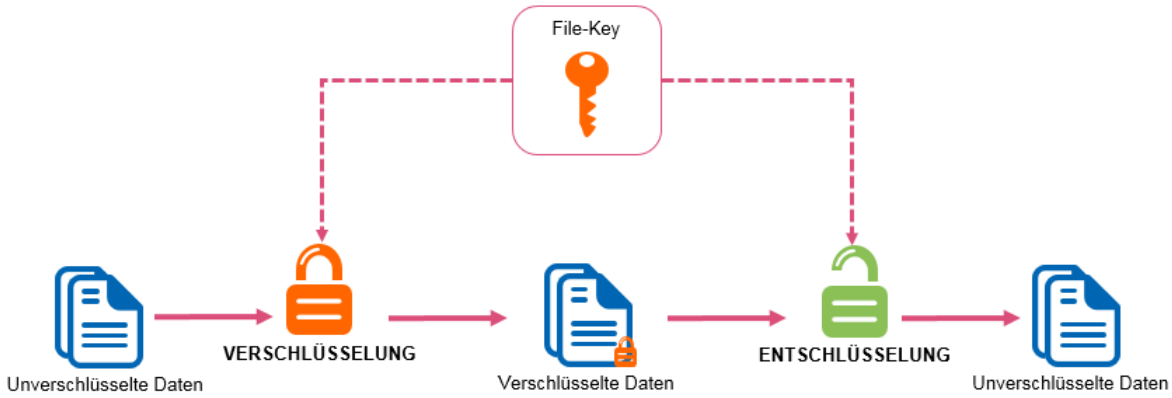
Die Implementierung der clientseitigen Verschlüsselung in agree21Doksharing basiert auf einer symmetrischen Verschlüsselung von Dateien mit einem individuellen File-Key. Dieser File-Key wird wiederum über eine asymmetrische Verschlüsselung mit Public/Private-Key Verfahren in agree21Doksharing abgelegt. In den folgenden Abschnitten wird die allgemeine Funktionsweise der Verschlüsselung entsprechend beschrieben.

1.1 Symmetrische Verschlüsselung

Das symmetrische Verfahren zur Verschlüsselung von Daten funktioniert über einen Schlüssel, ähnlich einem Passwort. Mit Hilfe dieses Schlüssels können Daten ver- und entschlüsselt werden. Im Rahmen von agree21Doksharing wird dieser Schlüssel als 'File-Key' bezeichnet.

Der Schlüssel muss beiden Parteien (Sender und Empfänger) bekannt sein, um einen verschlüsselten Austausch von Daten zu ermöglichen. Ohne diesen Schlüssel können die Daten jedoch nur durch extrem hohen Aufwand (Rechenleistung & Zeit) geknackt (unberechtigt entschlüsselt) werden. Die symmetrische Verschlüsselung gilt aufgrund der heute verfügbaren Algorithmen als sehr sicher und benötigt sowohl zur Ver- als auch zur Entschlüsselung verhältnismäßig wenig Rechenleistung, wenn der Schlüssel bekannt ist. Der bekannteste symmetrische Algorithmus ist AES - dieser wird auch im Rahmen von agree21Doksharing zur symmetrischen Verschlüsselung eingesetzt.

Schaubild: Ver- und Entschlüsselung mit einem symmetrischen Schlüssel



1.1.1 Beispiel: Die Sicherheitstür zum Archiv

Das Verfahren der symmetrischen Verschlüsselung lässt sich leicht begreifen, wenn Sie an einen Archiv-Raum denken, der über eine Sicherheitstür mit Zahlenschloss gesichert ist. Sie benötigen zum Betreten des Archivs eine Zahlenkombination.

Wenn Sie einer zweiten Person geheime Daten zugänglich machen wollen, öffnen Sie die Tür des Raums über eine Zahlenkombination, legen die Daten z. B. in einen Aktenschrank in diesem Raum und verlassen ihn wieder. Eine zweite Person möchte diese Daten nun entnehmen und muss dazu zuerst wieder den Raum betreten.

Sie gibt den gleichen Zahlencode an der Tür ein, betritt den Raum und kann auf die Daten zugreifen.

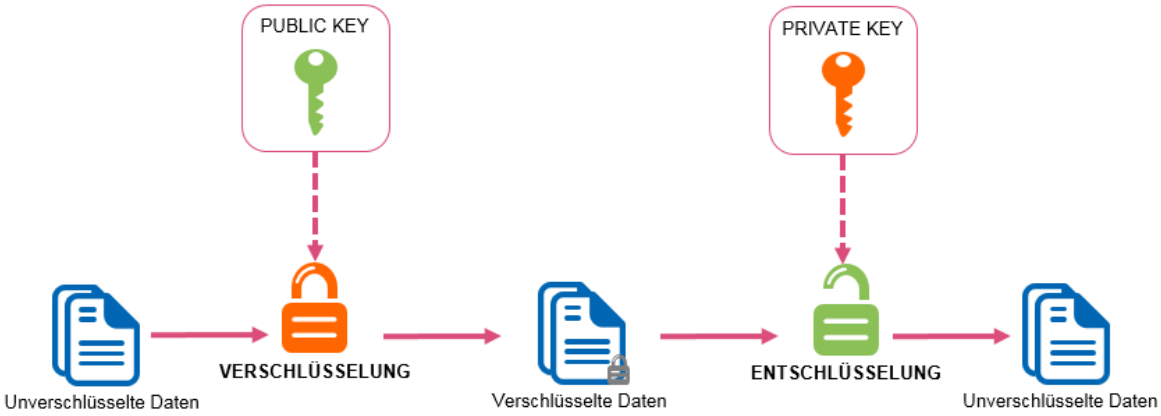
1.2 Asymmetrische Verschlüsselung

Das asymmetrische Verfahren kann sowohl zur Verschlüsselung als auch zur Signierung von Daten verwendet werden. Bei der asymmetrischen Verschlüsselung gibt es im Gegensatz zur symmetrischen Verschlüsselung immer zwei sich ergänzende Schlüssel:

- **Public Key:**
  Dieser Schlüssel wird zur Verschlüsselung von Daten verwendet.
- **Private Key:**
  Dieser Schlüssel wird zur Entschlüsselung von Daten verwendet.

Beide Schlüssel zusammen bilden ein Schlüsselpaar. Da die beiden Schlüssel nicht voneinander ableitbar sind, kann ein Schlüssel (der Public Key) öffentlich bekannt gegeben werden. Damit kann ein beliebiger Absender Daten verschlüsseln, diese jedoch nicht wieder entschlüsseln.

Schaubild: Ver- und Entschlüsselung mit einem asymmetrischen Schlüssel-Paar



Die Verschlüsselung des Klartextes erfolgt durch den öffentlichen Schlüssel (Public Key) in Kombination mit einem mathematischen Algorithmus, die Entschlüsselung durch den geheimen, zum Public Key passenden Private Key.

1.2.1 Beispiel 1: Der Briefkasten

Das Verfahren der asymmetrischen Verschlüsselung lässt sich leicht begreifen, wenn man an einen Briefkasten denkt. Jeder kann etwas einwerfen, weil der Briefkasten über eine Klappe Briefe entgegennimmt. Natürlich nur, wenn dem Einwerfenden der Standort des Briefkastens bekannt ist. Das ist sozusagen der Public Key. Zum Öffnen ist allerdings ein Schlüssel nötig, denn der Einwurfschlitz ist zu klein, um einen Brief einfach so entnehmen zu können.

Mit dem Public Key kann also jeder wie bei einem Briefkasten Daten sicher ablegen. Da aber nur der Empfänger über den geheimen Schlüssel (Private Key) verfügt, kann nur er die Daten aus dem Briefkasten entnehmen.

1.2.2 Beispiel 2: Multiplizieren

Die asymmetrische Verschlüsselung beruht auf mathematischen Verfahren, die in einer Richtung einfach aber in der anderen Richtung schwierig durchzuführen sind. Multiplizieren ist so ein Beispiel. Jeder kann einfach zwei Zahlen multiplizieren, z. B.:

3.121.163 * 4.811.953 = 15.018.889.661.339

Zahlen in Faktoren zu zerlegen, ist dagegen sehr mühselig: Wenn man erst einmal das Produkt hat, ist es sehr schwierig herauszufinden, aus welchen Faktoren dieses ursprünglich gebildet wurde. Verkürzt dargestellt entspricht der Public Key dem Produkt. Dieses wird benötigt, um Informationen für den Empfänger zu verschlüsseln. Dessen Private Key enthält die beiden Zahlen, aus denen das Produkt gebildet wurde. Diese sind für das Entschlüsselungsprogramm nötig, um die verschlüsselte Botschaft wieder lesbar zu machen.

1.2.3 Vorteile des Verfahrens

Das Problem des schwierigen Schlüsselaustausches ist dadurch elegant gelöst: Der öffentliche Teil kann jedem zugänglich gemacht werden, ohne dass die Sicherheit darunter leiden würde. Man benötigt schließlich immer den geheimen Schlüssel, um die Daten wieder zu entschlüsseln. Ein weiterer Vorteil des Verfahrens ist, dass sehr viel weniger Schlüssel benötigt werden als beim symmetrischen Verfahren, das schon für die Kommunikation von zwölf Personen untereinander 66 Schlüssel erfordert. Bei der asymmetrischen Verschlüsselung benötigt jeder nur ein Schlüsselpaar.

- Der größte Vorteil von Public-Key-Verfahren ist die hohe Sicherheit:
- Der Private Key zum Entschlüsseln verbleibt beim Besitzer. Dadurch trägt nur eine Person das Geheimnis.
- Die Schlüsselverteilung ist problemlos. Zum einen ist keine Übertragung des Private Keys durch unsichere Kanäle nötig. Zum anderen ist es ebenso nicht notwendig, den Public Key gegen Abhören zu härten, da er Angreifern wenig nützt.
- Das Brechen der Verschlüsselung, also das Entschlüsseln ohne den Private Key, kann Monate oder Jahre dauern. Bis dahin kann die Nachricht schon lange ihre Aktualität verloren haben. Obwohl der Algorithmus bekannt ist, ist der Rechen- und Zeitaufwand zu hoch, um das Verfahren zu brechen. Die heutzutage üblichen Schlüssel mit einer Länge von 2.048 Bit wurden faktisch noch nicht geknackt. 'Lediglich' Schlüssel mit einer Länge von 1.024 Bit konnte man mit extrem hohem Rechenaufwand nach einem Jahr Arbeit brechen.

Ein letzter Vorteil ist die Tatsache, dass die Schlüsselzahl nur linear zur Teilnehmerzahl wächst. Ergo werden viel weniger Schlüssel benötigt als bei der symmetrischen Verschlüsselung.

2 Verschlüsselung in agree21Doksharing

Die symmetrische Verschlüsselung benötigt im Vergleich zur asymmetrischen Verschlüsselung weniger Ressourcen (Leistung/Zeit) um einen bestimmten Grad an Sicherheit zu erreichen: Eine Datei muss z. B. nur einmal verschlüsselt werden, um sie mehreren Empfängern zugänglich zu machen. Nachteil dieser Methode ist jedoch, dass vor einem sicheren Datenaustausch der gemeinsame, geheime Schlüssel zwischen dem Sender und den Empfängern ausgetauscht werden muss.

Bei der asymmetrischen Verschlüsselung hingegen ist der Austausch eines gemeinsamen, geheimen Schlüssels nicht nötig, da zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet werden. Jeder Empfänger hat einen eigenen, öffentlichen Schlüssel der frei zugänglich gemacht werden kann. Herausforderung bei der asymmetrischen Verschlüsselung ist jedoch die Tatsache, dass Daten für jeden Empfänger individuell mit dessen Public Key verschlüsselt werden müssen. Hierdurch muss z. B. eine 1GB Datei vier Mal verschlüsselt werden, wenn vier Empfänger darauf zugreifen sollen. Die Verschlüsselung ist also ineffizienter, wenn es viele Empfänger gibt.

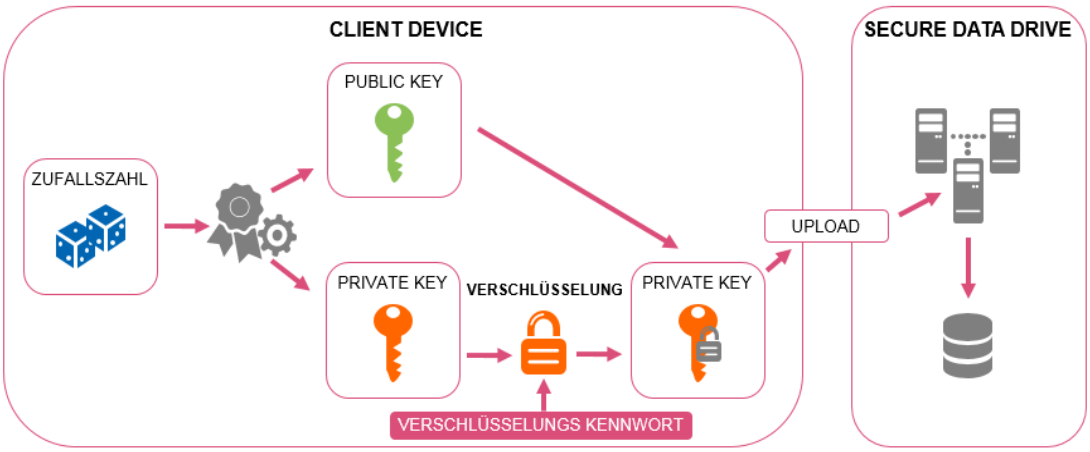
agree21Doksharing setzt daher auf eine Kombination aus beiden Verfahren: Jede Datei wird symmetrisch mit einem geheimen, individuellen Schlüssel, dem 'File-Key' verschlüsselt. Dieser Schlüssel wiederum wird asymmetrisch mit den Public Keys der Benutzer verschlüsselt, die auf die jeweilige Datei zugreifen sollen. Ein autorisierter Benutzer kann den File-Key mit Hilfe seines Private Key entschlüsseln und dann zur Entschlüsselung einer Datei verwenden.

Damit muss jede Datei auch bei mehreren berechtigten Nutzern nur einmal verschlüsselt werden, die Sicherheit der individuellen Schlüssel pro Benutzer ist jedoch weiterhin gegeben.

2.1 Generierung der Schlüsselpaare

Jeder Benutzer einer Instanz von agree21Doksharing, auf der vom jeweiligen Data Drive Admin die **Triple-CryptTM** Technologie aktiviert wurde, wird bei seinem nächsten Login in den Web-Client aufgefordert, sein Verschlüsselungskennwort festzulegen.

Schaubild: Generierung der Schlüsselpaare



Sobald der Benutzer sein Verschlüsselungskennwort eingegeben hat, wird auf seinem Endgerät unter Einbeziehung einer dort generierten Zufallszahl ein asymmetrisches Schlüsselpaar mit einer Schlüssellänge von jeweils mindestens 2.048 Bit (RSA2048) generiert. Der Private Key wird im

nächsten Schritt lokal am Endgerät des Benutzers mit dem Verschlüsselungskennwort des Benutzers symmetrisch verschlüsselt (AES256/CBC). Anschließend werden der Public Key sowie der verschlüsselte Private Key auf agree21Doksharing übertragen und dort in der Datenbank abgelegt.

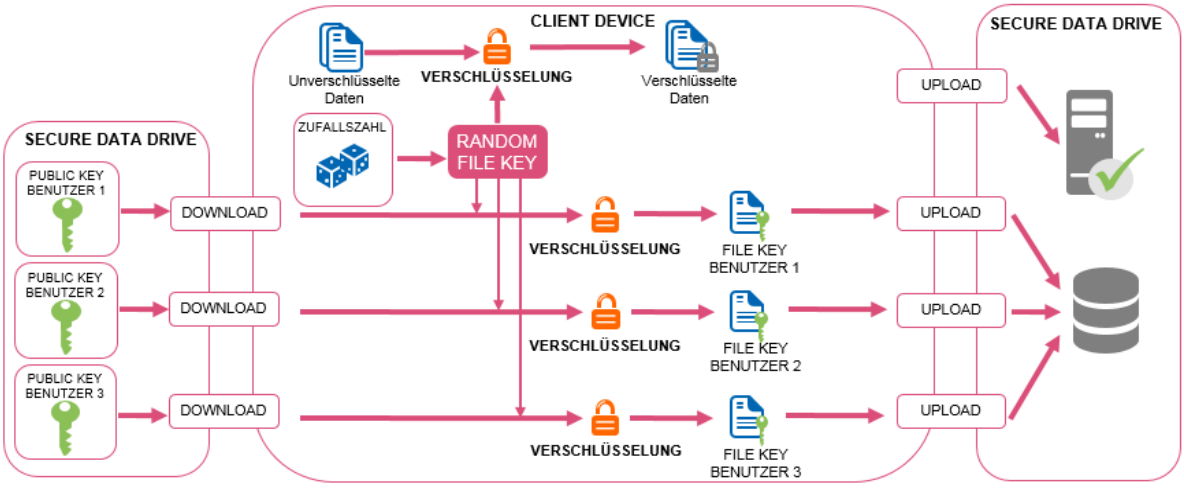
Wichtig: Das Verschlüsselungskennwort hat bei diesem Prozess das Endgerät des Benutzers niemals verlassen. Dieser Grundsatz gilt selbstverständlich für alle Aktionen, die in Zusammenhang mit der clientseitigen Verschlüsselung stehen.

2.2 Hochladen von Dateien in verschlüsselte Datenräume

Lädt ein Benutzer Dateien in einen verschlüsselten Datenraum hoch, so werden zuerst die Public Keys aller Benutzer, die Zugriff auf diesen Datenraum haben, auf das Endgerät des Benutzers heruntergeladen.

Anschließend wird auf dem Endgerät des Benutzers ein Random File-Key (256 Bit) für die hochzuladende Datei generiert. Danach wird diese Datei mit dem Random File-Key symmetrisch verschlüsselt (AES256/GCM) und in verschlüsselter Form zu agree21Doksharing übertragen.

Schaubild: Hochladen von Dateien in verschlüsselte Datenräume



Für jeden Benutzer, der Zugriff auf den verschlüsselten Datenraum mit der neu hochgeladenen Datei hat, muss der File-Key mit dem Public-Key des jeweiligen Benutzers asymmetrisch verschlüsselt und in der Datenbank von agree21Doksharing abgelegt werden.

Diese Zugriffsschlüssel - die BenutzerFileKeys - können bei Bedarf im Hintergrund erzeugt werden. Der Upload einer Datei erfordert somit nur die Bereitstellung einiger weniger (mindestens jedoch eines) BenutzerFileKeys. Sobald diese Bedingung erfüllt ist, kann der Benutzer mit dem agree21Doksharing bereits wieder arbeiten, obwohl unter Umständen noch eine große Anzahl an Verschlüsselungsoperationen ausstehen. Diese können einfach im Hintergrund durchgeführt werden, ohne dass es zu Behinderungen kommt. Besonders interessant ist diese Bereitstellung von BenutzerFileKeys dann, wenn ein Sync-Client zum Einsatz kommt, da diese Anwendungen auf Systemen mit ausreichend Leistung laufen.

Zudem entlastet dieses Vorgehen auch die mobilen Apps, da ein Benutzer, der eine verschlüsselte Datei in ein agree21Doksharing lädt, nun nicht mehr die asymmetrischen Schlüssel für alle anderen Benutzer bereitstellen muss.

Er muss lediglich darauf achten, dass er die BenutzerFileKeys für einige wenige Benutzer erzeugt, die diese in der Folge ihrerseits an die restlichen Berechtigten weiter verteilen können. z. B. über Clients mit mehr Ressourcen (CPU-Leistung und Bandbreite).

Besonders interessant an dieser Lösung ist, dass auch Benutzer in verschlüsselten Datenräumen berechtigt werden können, die noch kein Verschlüsselungskennwort festgelegt haben (= noch kein Schlüsselpaar besitzen), und es somit noch nicht möglich ist, für sie BenutzerFileKeys zu erzeugen. Die betroffenen Teilnehmer erhalten bei einem versuchten Zugriff auf den Datenraum die Aufforderung, ein Verschlüsselungskennwort festzulegen. Sobald dieses vorhanden ist, können andere Benutzer, die bereits Zugriff auf die verschlüsselten Dateien haben, für diese Dateien (automatisch oder manuell ausgelöst) die fehlenden Schlüssel bereitstellen. So erhält der berechtigte Nachzügler innerhalb absehbarer Zeit vollständigen Zugriff auf alle vorhandenen Dateien - ohne Wartezeit für einen der aktiven Nutzer.

2.3 Herunterladen von Dateien aus verschlüsselten Datenräumen

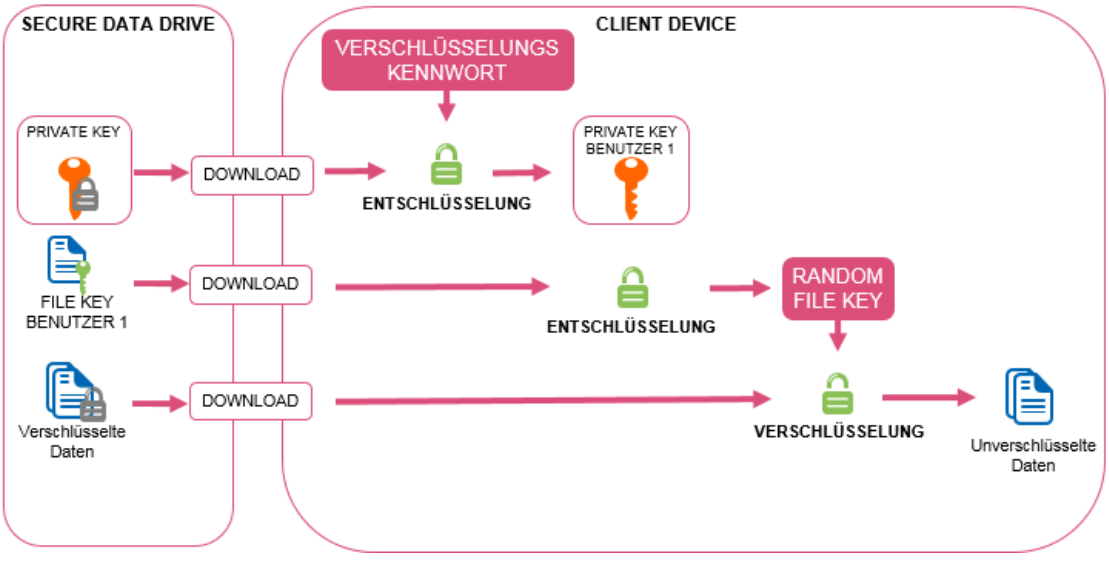
Will ein Benutzer eine verschlüsselte Datei aus agree21Doksharing herunterladen, wird zuerst sein verschlüsselter Private Key heruntergeladen und der Benutzer wird zur Eingabe seines Verschlüsselungskennworts aufgefordert.

Mit diesem Verschlüsselungskennwort wird der Private Key des Benutzers lokal auf seinem aktuellen Endgerät entschlüsselt.

Im nächsten Schritt wird der Benutzer-File-Key auf den Client heruntergeladen, der beim Upload der Datei genau für diese Datei und für diesen Benutzer erzeugt wurde. Dieser Benutzer-File-Key wird mit dem entschlüsselten Private Key des Benutzers entschlüsselt, sodass der beim Upload zur Verschlüsselung der Datei verwendete Random File-Key auf dem Client im Klartext vorliegt.

Anschließend wird die symmetrisch verschlüsselte Datei auf das Endgerät heruntergeladen und dort mit dem entschlüsselten Random File-Key entschlüsselt, wonach die entschlüsselte Datei auf dem Client geöffnet oder gespeichert werden kann.

Schaubild: Herunterladen von Dateien aus verschlüsselten Datenräumen



2.4 Hinzufügen von Benutzern zu verschlüsselten Datenräumen

Für jeden Benutzer, der Zugriff auf einen verschlüsselten Datenraum hat, und für jede Datei in diesem Datenraum, existiert ein eigener Benutzer-File-Key, mit dessen Hilfe die jeweilige Datei entschlüsselt werden kann.

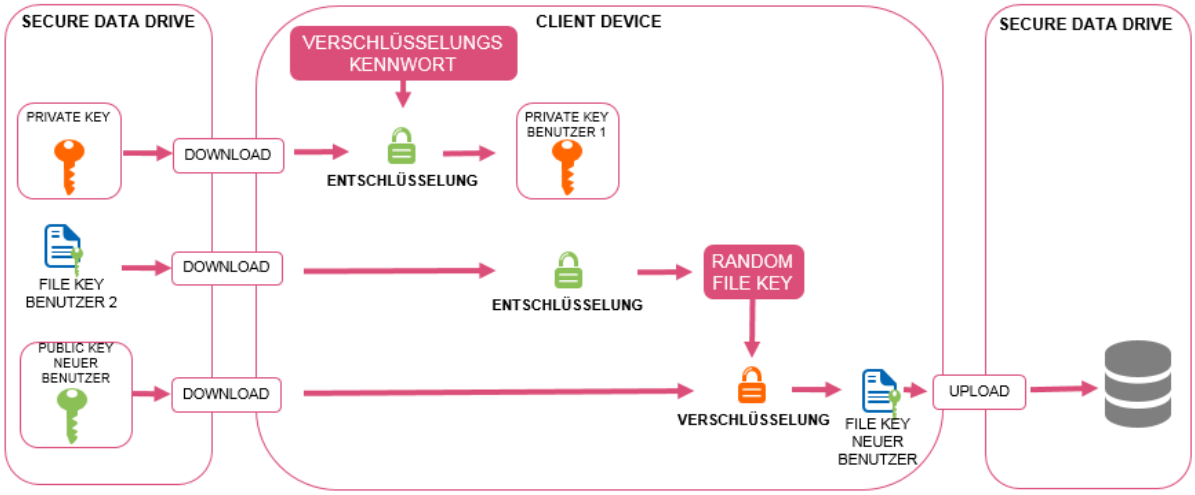
Soll später ein weiterer Benutzer Zugriff auf diesen verschlüsselten Datenraum erhalten, so muss für diesen Benutzer für jede Datei, die in diesem Datenraum abgelegt ist, nachträglich ein Benutzer-File-Key generiert werden.

Um dies zu bewerkstelligen, werden zum Zeitpunkt des Hinzufügens des neuen Benutzers durch einen Datenraum Admin die Benutzer-File-Keys des entsprechenden Datenraum Admins auf dessen Endgerät heruntergeladen und dort nach Eingabe des Verschlüsselungskennworts des Datenraum Admins soweit entschlüsselt, dass der jeweilige Random File-Key der Datei zugänglich ist. Aus dem entschlüsselten Random File-Key der jeweiligen Datei und dem Public Key des hinzuzufügenden Benutzers wird ein neuer Benutzer-File-Key für den neuen Benutzer erstellt und nach agree21Doksharing übertragen.

Dadurch wird sichergestellt, dass der neue Benutzer für jede verschlüsselte Datei in diesem Datenraum einen eigenen Benutzer-File-Key hat, mit dem er die Datei entschlüsseln kann.

Da hierzu je nach Anzahl an Dateien eine entsprechende Rechenleistung benötigt wird, steht dieses Feature ausschließlich im Web-Client oder den Desktop-Clients zur Verfügung und sollte über ein vollwertiges Endgerät (PC, Notebook etc.) aufgerufen werden.

Schaubild: Hinzufügen von Benutzern zu verschlüsselten Datenräumen



3 Sondersituationen

3.1 Zurücksetzen des Verschlüsselungskennworts

Hat ein Benutzer sein Verschlüsselungskennwort vergessen, kann er seinen Private Key nicht mehr entschlüsseln, wodurch eine Entschlüsselung der BenutzerFileKeys und somit der verschlüsselten Dateien unmöglich wird. Das Verschlüsselungskennwort kann aus Sicherheitsgründen auch nicht einfach geändert werden.

Zum Ändern / Zurücksetzen des Verschlüsselungskennworts muss sich der Benutzer zuerst ganz normal in agree21Doksharing anmelden. In seinem Benutzerprofil kann er dann sein Verschlüsselungskennwort zurücksetzen/ändern.

Hierbei wird als erster Schritt das Verschlüsselungskennwort des Benutzers gelöscht. Die sich ergebende Kette an Aktionen stellt sich wie folgt dar:

- Sowohl Public Key als auch Private Key des Benutzers werden aus agree21Doksharing gelöscht.
- Alle Benutzer-File-Keys dieses Benutzers werden aus agree21Doksharing gelöscht.
- Der Benutzer wird aus allen verschlüsselten Datenräumen entfernt, auf die er Zugriff hat.

Der Benutzer hat dadurch vorerst keinerlei Zugriff mehr auf verschlüsselte Datenräume und deren Inhalte. Daher wird als nächster Schritt vom Benutzer ein neues Verschlüsselungskennwort vergeben, wodurch wie im **Kapitel Generierung der Schlüsselpaare** ein neues Schlüsselpaar für diesen Benutzer erzeugt wird.

Im Verlauf des Zurücksetzens wird dem Benutzer zudem eine Liste der verschlüsselten Datenräume angezeigt, auf die er bisher Zugriff hatte. Um wieder Zugriff auf diese verschlüsselten Datenräume und die darin enthaltenen Dateien zu erlangen, muss der Benutzer die jeweiligen Datenraum Admins kontaktieren und sich von diesen neu zu den jeweiligen Datenräumen hinzufügen lassen, wodurch der in **Kapitel Hinzufügen von Benutzern zu verschlüsselten Datenräumen** dargestellte Prozess ausgelöst wird.

3.2 Verwendung von Rescue Keys

agree21Doksharing bietet zudem die Möglichkeit, über sogenannte Rescue Keys eine Entschlüsselung von Dateien möglich zu machen, falls alle Benutzer ihre Verschlüsselungskennwörter vergessen haben sollten. Diese Rescue Keys sind generell kundenbezogen und der Fiducia & GAD nicht bekannt.

Aktiviert ein berechtigter Datenraum Admin eines Kunden in einem seiner Datenräume die Verschlüsselung, kann er eine von drei Fallback-Methoden wählen:

- **Data Drive Rescue Key:**
  Alle Dateien sind in diesem Datenraum mit dem Data Drive Rescue Key des Kunden entschlüsselbar.

- **Datenraum Rescue Key:**
  Die Dateien sind in diesem Datenraum nicht mit dem Data Drive Rescue Key entschlüsselbar, sondern lediglich mit dem Datenraum Rescue Key genau dieses Datenraums.

- **Kein Rescue Key:**
  Dateien sind ausschließlich durch die Nutzer dieses Datenraums entschlüsselbar und es besteht ansonsten keinerlei Fallback-Mechanismus, um die Dateien anderweitig entschlüsseln zu können. Bei Verlust der Private-Keys der Raum-Nutzer oder wenn die entsprechenden, persönlichen Verschlüsselungskennwörter nicht mehr bekannt sind, kann nicht mehr auf die Daten des Raums zugegriffen werden.

Die Funktionsweise der beiden Rescue Keys ist in den folgenden Kapiteln näher beschrieben.

3.2.1 Data Drive Rescue Key

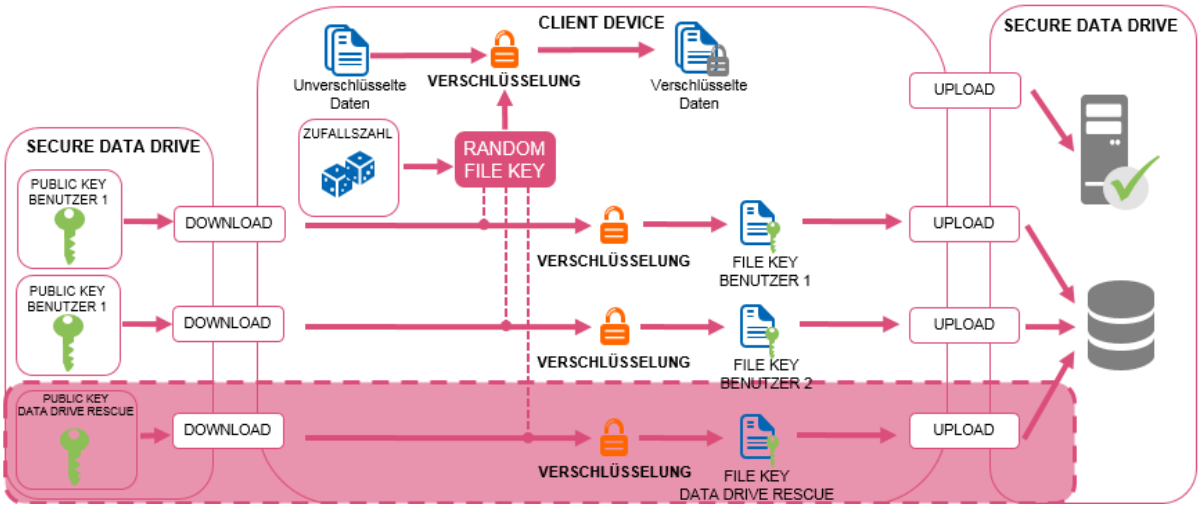
Aktiviert ein Data Drive Admin eines Endkunden in seiner Instanz von agree21Doksharing die **Triple-CryptTM Technologie**, wird er zur Eingabe des gewünschten Data Drive Rescue Keys aufgefordert.

Dadurch wird im agree21Doksharing des Kunden ein unsichtbarer System-Benutzer angelegt, für den analog zu Kapitel Generierung der Schlüsselpaare (S. 7) ein Schlüsselpaar generiert wird, wobei der vom Data Drive Admin festgelegte Data Drive Rescue Key als Verschlüsselungskennwort verwendet wird.

Bei der Aktivierung der Verschlüsselung für einen Datenraum durch einen berechtigten Datenraum Admin wird dieser gefragt, ob alle Dateien in diesem Raum ebenfalls mit dem Data Drive Rescue Key verschlüsselt werden sollen, sodass diese Dateien ebenfalls mit dem Data Drive Rescue Key entschlüsselt werden können.

Wenn dies gewünscht wird, so wird für alle Dateien in diesem Datenraum jeweils ein eigener Benutzer-File-Key erstellt, der auf dem Public Key des unsichtbaren System-Benutzers für den Data Drive Rescue Key basiert.

Schaubild: Data Drive Rescue Key



In der Folge können alle Dateien in diesem Datenraum auch durch Eingabe des Data Drive Rescue Keys entschlüsselt werden.

3.2.2 Datenraum Rescue Key

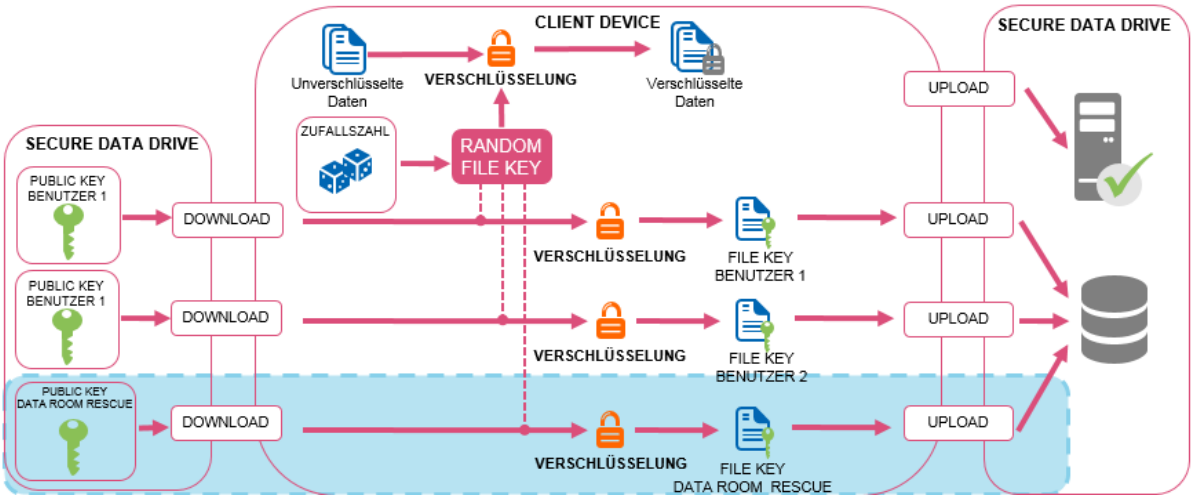
Aktiviert ein berechtigter Datenraum Admin eines Endkunden in einem seiner Datenräume die Verschlüsselung, muss er sich für eine von drei zuvor genannten Fallback-Methoden entscheiden.

Wählt er die Verwendung eines speziellen Datenraum Rescue Keys, der nur für diesen speziellen Datenraum verwendet wird, wird er zur Eingabe des gewünschten Datenraum Rescue Keys aufgefordert.

Dadurch wird in agree21Doksharing des Kunden ein weiterer, unsichtbarer System-Benutzer angelegt, für den analog zu **Kapitel Generierung der Schlüsselpaare** ein Schlüsselpaar generiert wird, wobei der vom Datenraum Admin festgelegte Datenraum Rescue Key als Verschlüsselungskennwort verwendet wird.

Anschließend wird für alle Dateien in diesem Datenraum jeweils ein eigener Benutzer-File-Key erstellt, der auf dem Public Key des unsichtbaren System-Benutzers für den Datenraum Rescue Key basiert.

Schaubild: Datenraum Rescue Key



In der Folge können alle Dateien in diesem Datenraum auch durch Eingabe des Datenraum Rescue Keys entschlüsselt werden.