Ende-zu-Ende-Verschlüsselung

in netfiles Data Vault

Inhalt

1. Einleitung

Ende-zu-Ende-Verschlüsselung („*End-to-End Encryption*“, *E2EE*) ermöglicht es Benutzern, Informationen unabhängig vom Kommunikationskanal sicher auszutauschen. Nachrichten und Informationen werden auf dem jeweiligen Eingabe- oder Empfangsgerät ver- und entschlüsselt – vor bzw. nach der Übertragung. Dadurch sind sie auf dem gesamten Übertragungsweg durchgehend geschützt.

Dieses Dokument präsentiert Ihnen einen kompakten Überblick darüber, wie netfiles Ende-zu-Ende-Verschlüsselung in netfiles Data Vault implementiert hat, sodass:

- Dokumentinhalte, Kommentare und Anmerkungen ausschließlich verschlüsselt auf den Servern von netfiles ankommen;
- die Ver- und Entschlüsselung dieser Dokumentinhalte, Kommentare und Anmerkungen ausschließlich auf dem Gerät des Nutzers (im Browser oder in der netfiles App) erfolgt;
- die für die Verschlüsselung verwendeten Schlüssel niemals auf den Servern von netfiles so gespeichert werden, dass es netfiles möglich wäre, sie zur Entschlüsselung von Inhalten, Kommentaren oder Anmerkungen zu verwenden;
- all dies zusätzlich zu der derzeitigen Verschlüsselung des Datenraums und der für die Kommunikation mit den Servern von netfiles verwendeten TLS-Verschlüsselung geschieht.

2. Voraussetzungen

Ende-zu-Ende-Verschlüsselung (E2EE) ist eine starke Schutzmaßnahme für die sensibelsten Daten eines Unternehmens. Da die Ver- und Entschlüsselung von Daten ausschließlich auf dem jeweiligen Endgerät der Benutzer stattfinden, sind dadurch bedingt einige Produktivitäts-Funktionen nicht oder nur eingeschränkt verfügbar. Der Grund dafür ist, dass diese Funktionen – zum Beispiel Virenscanner oder die Online-Bearbeitung von Dokumenten – serverseitig stattfinden und kurzfristig Zugriff auf unverschlüsselte Daten benötigen.

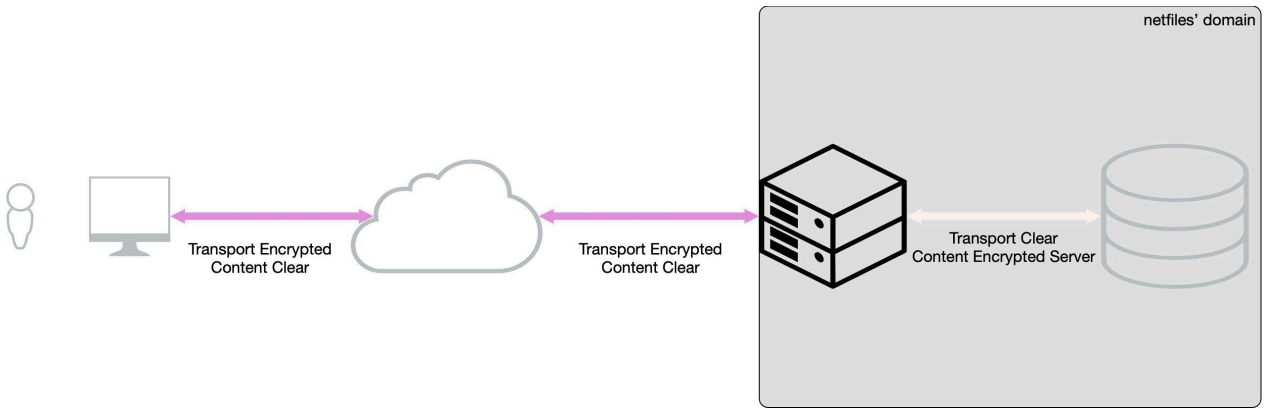
Für welche Daten sollte netfiles Data Vault genutzt werden?

Der Einsatz von netfiles Data Vault wird empfohlen, wenn der Schutzbedarf für die betroffenen Daten dies unbedingt erfordert. Unabhängig von E2EE erfüllt netfiles höchste Sicherheitsstandards, ist nach ISO 27001 und SOC-2 zertifiziert, BSI-C5-testiert und wird regelmäßig von unabhängiger Stelle auf Schwachstellen geprüft (Pentest). Die Übertragung und Speicherung von Daten auf netfiles Servern erfolgt immer AES-256-verschlüsselt.

Für weitere Informationen zum allgemeinen Schutzstandard von netfiles empfehlen wir Ihnen unser ausführliches Sicherheitskonzept.

3. Übersicht

Die Ende-zu-Ende-Verschlüsselung in netfiles Data Vault ist eine Ergänzung zur bestehenden und standardmäßigen Verschlüsselung von netfiles Datenräumen. Auch ohne E2EE sind Daten in netfiles immer mit Transportverschlüsselung („Encryption-in-Transit“) sowie während der Speicherung („Encryption-at-Rest“) geschützt:



Transportverschlüsselung

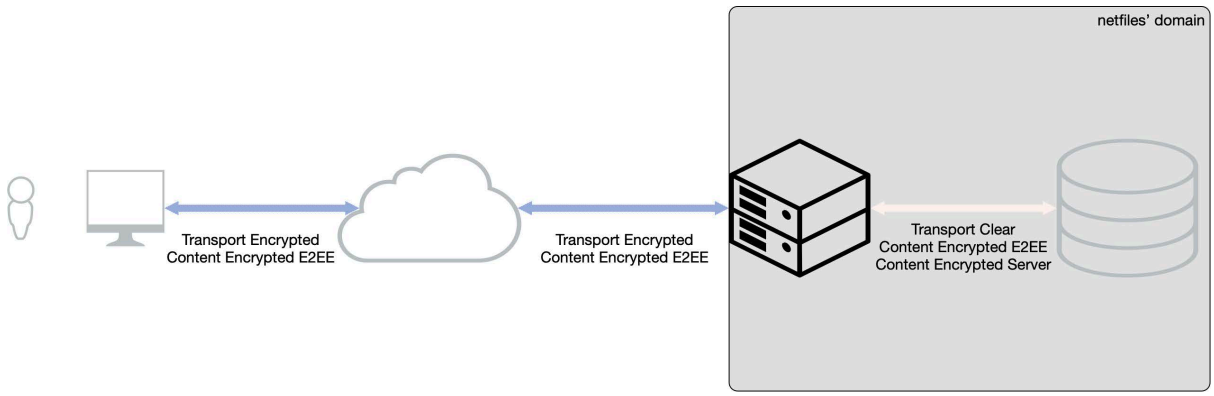
Die Inhalte, die vom Computer des Nutzers hoch- oder heruntergeladen werden, werden über eine TLS-Verbindung an die Server von netfiles übertragen. Die TLS-Verbindung verschlüsselt die gesamte Kommunikation mit den netfiles Servern. So kann ein Außenstehender weder sehen, was transportiert wird, noch den transportierten Inhalt verändern.

Ruheverschlüsselung

Daten werden auf den netfiles Servern nur in verschlüsselter Form gespeichert. Dazu versieht netfiles alle eingehenden Daten mit AES-256-Verschlüsselung. Eine Entschlüsselung findet nur im Rahmen der angebotenen, serverseitigen Dienste (zum Beispiel durch den Virenscanner und für die Online-Bearbeitung von Dokumenten) statt.

Ende-zu-Ende-Verschlüsselung

In netfiles Data Vault werden die Inhalte bereits auf dem Endgerät des Benutzers verschlüsselt und erst im Anschluss daran an den Server übertragen. Der Transport ist standardmäßig mit TLS gesichert. Sobald der Inhalt auf den Servern von netfiles ankommt, wird er automatisch erneut verschlüsselt und in der Datenbank von netfiles gespeichert.



Die Verschlüsselung vor dem Hochladen und Entschlüsselung nach dem Herunterladen von E2EE-Daten findet vollständig im Hintergrund statt („On-the-fly-Verschlüsselung“) und erfordert nach der Anmeldung und Eingabe des persönlichen Daten-Schlüssels im verschlüsselten Datenraum keine weiteren Aktionen auf Benutzerseite.

Wichtig: Da die Inhalte bereits verschlüsselt auf den netfiles Servern ankommen und diese keinen Zugriff auf den E2EE-Schlüssel haben, kann keine der serverseitigen Funktionen (zum Beispiel der Virenscanner und die Online-Bearbeitung von Dokumenten), die Zugriff auf die unverschlüsselten Inhalte erfordern, ausgeführt werden.

4. Implementierung

Die gesamte Verschlüsselung inklusive aller dazugehörigen Prozesse (z. B. das Schlüsselmanagement) finden vollständig im Hintergrund statt und erfordern kein technisches Know-how des Benutzers. Der Benutzer wird während der Einrichtung (bzw. dem erstmaligen Betreten) eines netfiles Data Vault dazu aufgefordert, ein sicheres Passwort für die Nutzung der Ende-zu-Ende-Verschlüsselung (E2EE) zu vergeben. Dieser „Daten-Schlüssel“ wird als Ausgangspunkt für alle Verschlüsselungs-Maßnahmen verwendet.

Um E2EE in netfiles Data Vault anzubieten, übernimmt netfiles folgende Aufgaben:

- Verschlüsseln/Entschlüsseln von Inhalten im Browser mit einem AES-256-Schlüssel, um die Vertraulichkeit und Integrität der Inhalte zu gewährleisten
- Den für die Ver-/Entschlüsselung verwendeten Schlüssel an einem sicheren Ort speichern, auf den auch netfiles keinen Zugriff hat
- Den für die Ver-/Entschlüsselung verwendeten Schlüssel auf sichere Weise an neue Mitglieder des Datenraums weitergeben

netfiles verwendet dafür folgende Verfahren und Technologien:

- RSA-4096: Schlüsselaustausch (privater & öffentlicher Schlüssel)
- Argon2id: Schlüssel-Ableitung
- AES-GCM: Symmetrische Verschlüsselung (Daten-Verschlüsselung), einschließlich Integritätsprüfung
- WebCrypto: Zur Erzeugung eines asymmetrischen RSA 4096-Bit-Schlüsselpaares, zur Schlüsselverwaltung und zur Ver-/Entschlüsselung

Für die Ver- und Entschlüsselung sowie die Schlüsselgenerierung verwendet netfiles WebCrypto sowie die Bibliothek Argon2id. Da WebCrypto aktuell noch keine Schlüsselableitung mit Argon2id unterstützt (Stand: März 2025), verwendet netfiles daher die WebAssembly-Version der Argon2id-Bibliothek.

RSA-Schlüsselpaar: Öffentlicher und privater Schlüssel („Daten-Schlüssel“)

Um E2EE-Daten mit Benutzern und Gruppen teilen zu können, sind ein privater („*Private Key*“) und öffentlicher („*Public Key*“) Schlüssel erforderlich. Während der private Schlüssel ausschließlich dem Benutzer bekannt sein darf und zur Entschlüsselung benötigt wird, ist der öffentliche Schlüssel frei verfügbar und wird nur für die Verschlüsselung genutzt. Sowohl der Administrator als auch die zukünftigen Benutzer eines netfiles Data Vault benötigen ein RSA-Schlüsselpaar. Dieses wird beim Erstellen des Datenraumes (Administrator) oder infolge einer Einladung in einen Datenraum (Benutzer) angelegt.

Wenn der Administrator erstmalig ein netfiles Data Vault anlegt, generiert netfiles mithilfe von WebCrypto (crypto.subtle.generateKey(...)) ein RSA-Schlüsselpaar mit einer Länge von 4096 Bit. Der originale, private RSA-Schlüssel wird mit einem Passwort geschützt, das hierfür vom Administrator festgelegt werden muss. Dieses ausschließlich für E2EE verwendetes Passwort, ist der persönliche „*Daten-Schlüssel*“.

Aus dem Daten-Schlüssel werden hierzu ein AES-256-Schlüssel („*Passwort-Schlüssel*“) und Initialisierungsvektor (IV) abgeleitet, die zur Verschlüsselung des privaten RSA-Schlüssels verwendet werden. Der so verschlüsselte private Schlüssel und der öffentliche Schlüssel werden im Anschluss im Konto des Benutzers gespeichert.

Sicherheits-Hinweis: Die Verwendung von RSA-4096 und Argon2id erfordert aufgrund der benötigten Rechenleistung moderne Computer oder Mobilgeräte. Dennoch hat sich netfiles für deren Verwendung entschieden: RSA-2048 wurde vom deutschen BSI ab 2025 als unsicher eingestuft und auch die verbreitete Empfehlung (RSA-3072) erscheint nur als Übergangslösung. Wir gehen davon aus, dass RSA-4096 weit über das Jahr 2035 hinaus, bis mindestens in die 2040er Jahre hinein, sicher genug sein wird.

Sollten sich die Sicherheitsempfehlungen vorzeitig ändern, ermöglicht unsere Implementierung einen einfachen Wechsel von RSA-4096 zu einem noch höheren Verfahren.

Wichtig: Der persönliche Daten-Schlüssel ist *unabhängig* vom netfiles Benutzer-Kennwort, das zur Anmeldung bei netfiles erforderlich ist. Aus Sicherheitsgründen sollte auf keinen Fall dasselbe Passwort als Benutzer-Kennwort und Daten-Schlüssel verwendet werden. Der Daten-Schlüssel ist (neben den netfiles Zugangsdaten) das einzige Passwort, das im weiteren Verlauf von Administrator und Benutzern gemerkt oder gespeichert werden muss.

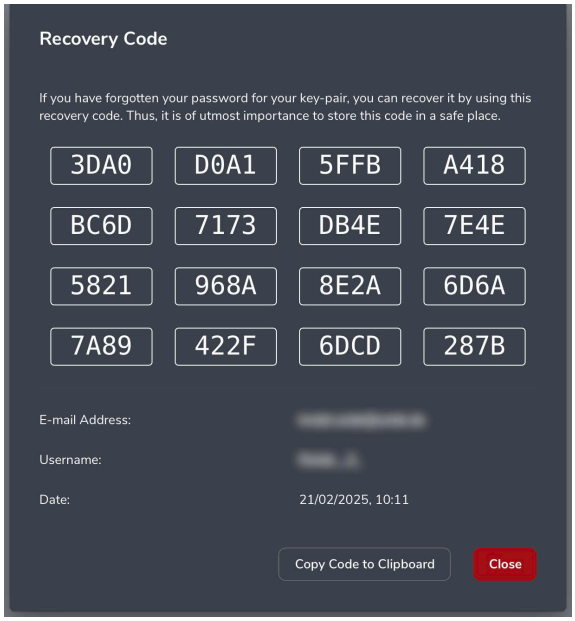
Alle weiteren für die Arbeit mit E2EE-Daten erforderlichen Prozesse werden von netfiles im Hintergrund abgewickelt. Der Daten-Schlüssel ist für jeden Benutzer von netfiles einmalig und kann für mehrere unterschiedliche Datenräume genutzt werden. Er muss daher nur beim erstmaligen Anlegen/Betreten eines netfiles Data Vault erstellt werden.

Wiederherstellungs-Code

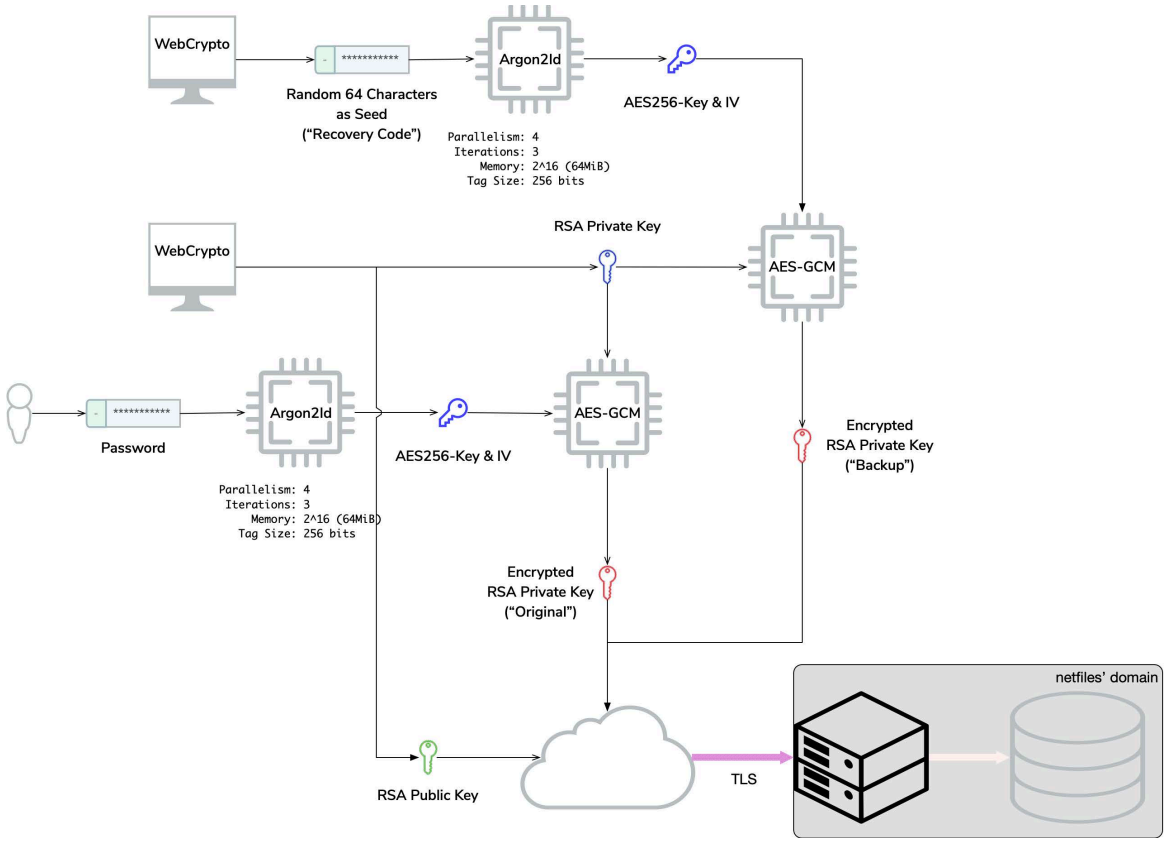
Da netfiles zu keinem Zeitpunkt den persönlichen Daten-Schlüssel von Benutzern – d.h. das für die Entschlüsselung von E2EE-geschützten Daten erforderliche Passwort – kennt, würde dessen Verlust auch die Daten unwiederbringlich verschließen. Als Sicherheit wird deshalb bereits beim Anlegen der Verschlüsselung ein Wiederherstellungsschlüssel für den Nutzer angelegt.

Dazu wird bei der Ableitung des Passwort-Schlüssels aus dem vom Benutzer gewählten Passwort zusätzlich eine zufällige Folge aus 64 Hex-Zeichen („*Wiederherstellungs-Code*“) als Seed für eine weitere Argon2id-Ableitung generiert. Daraus werden je ein weiterer AES-256-Schlüssel („*Wiederherstellungs-Schlüssel*“) und ein IV erzeugt.

Der (unverschlüsselte) private Schlüssel des Benutzers wird mit diesem Wiederherstellungs-Schlüssel und IV verschlüsselt und als Backup gespeichert. Der Wiederherstellungs-Code wird an den Benutzer zur sicheren Aufbewahrung übergeben. Der private RSA-Schlüssel so mit dem Wiederherstellungs-Code weiterhin entschlüsselt werden, falls der Benutzer das für die Entschlüsselung des privaten RSA-Schlüssels (und damit aller damit verschlüsselten Daten) erforderliche Passwort – also seinen persönlichen Daten-Schlüssel – vergisst oder verliert.



Übersicht: Schlüssel-Erstellung und -speicherung bei netfiles Data Vault

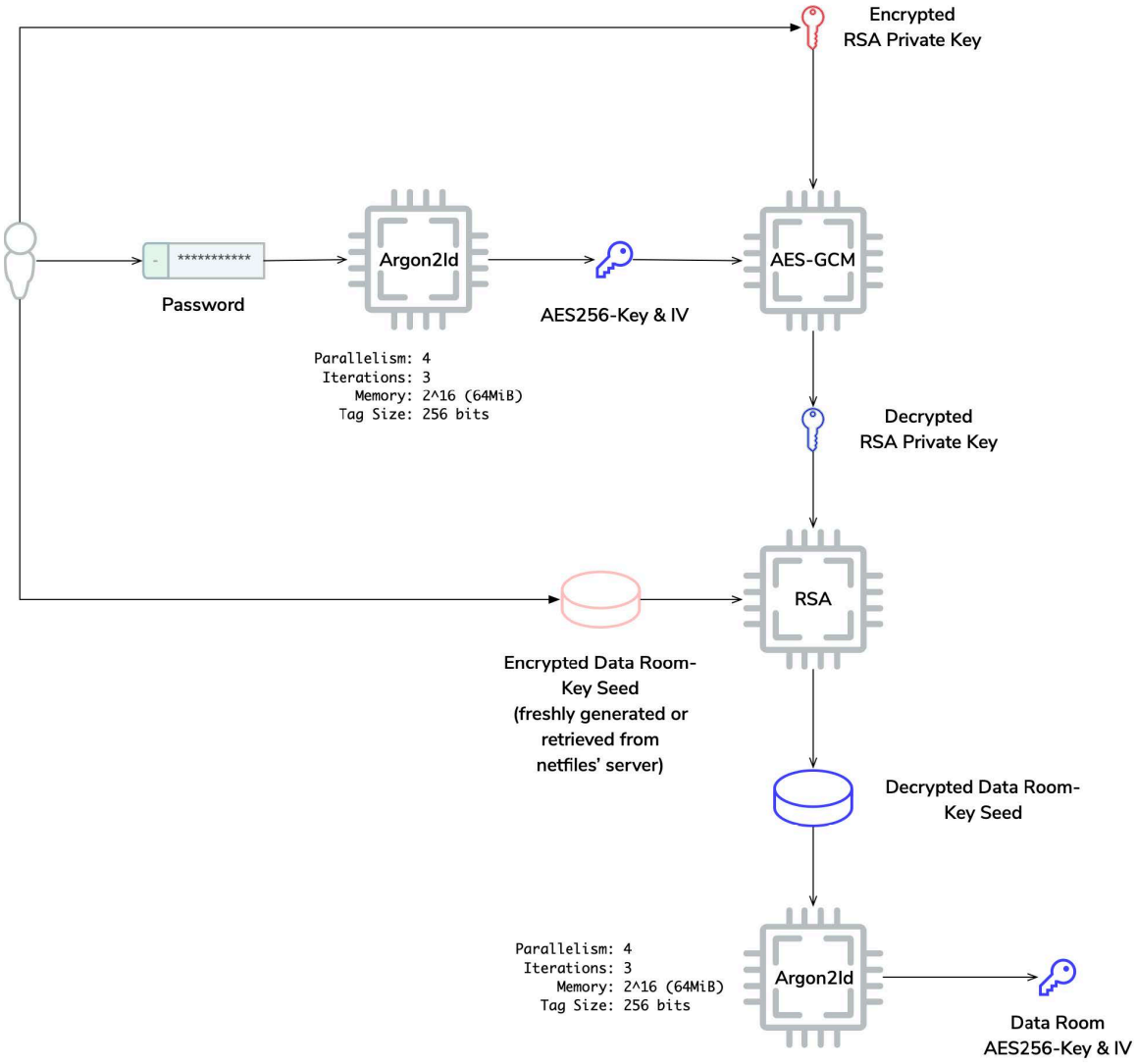


AES-Datenraum-Schlüssel

Für die Verschlüsselung der Daten in einem Datenraum generiert netfiles einen zufälligen, 32 Byte großen Seed mit WebCrypto (crypto.getRandomValues(new Uint8Array(32))). Die hexadezimale Darstellung dieser Zufallswerte wird von nun an als Seed („*Datenraum-Schlüssel-Seed*“) in Argon2Id verwendet, um den eigentlichen AES-256-Schlüssel und IV („*Datenraum-Schlüssel*“) zur **Ver- und Entschlüsselung von Datenrauminhalten** zu generieren.

netfiles verschlüsselt den Datenraum-Schlüssel-Seed unmittelbar mit dem öffentlichen Schlüssel des Administrators und speichert ihn in dessen Benutzerkonto für diesen Datenraum. Anschließend löscht netfiles den ursprünglichen, unverschlüsselten Datenraum-Schlüssel-Seed , um ihn nicht länger als notwendig im Arbeitsspeicher zu behalten. Für jede Sitzung wird (lokal im Browser) ein für den Zeitraum dieser Sitzung gültiger Datenraum-Schlüssel erzeugt.

Für jede zukünftige Verwendung des Datenraum-Schlüssel-Seeds folgt netfiles folgendem Ablauf, um ihn abzurufen:



Bitte beachten Sie: Der generierte AES-Datenraum-Schlüssel sowie IV werden sofort in WebCrypto zur Ver-/Entschlüsselung mit exportable: false importiert. Dies gilt auch für den privaten Schlüssel des Benutzers: Sobald dieser entschlüsselt wurde, importiert netfiles ihn unmittelbar in WebCrypto zur weiteren Verwendung und löscht die unverschlüsselte Version, um sie nicht länger als nötig im Arbeitsspeicher zu halten.

Von nun an werden alle Inhalte, Kommentare und Anmerkungen automatisch mit AES-256 im Browser des Administrators (oder eingeladener Benutzer) verschlüsselt, bevor sie an den Server gesendet werden. Um einen Inhalt, Kommentar oder Anmerkung zu öffnen oder herunterzuladen, werden diese ebenfalls im Browser entschlüsselt, nachdem sie vom Server abgerufen wurden. Der gesamte Prozess der Ver- und Entschlüsselung ist für den Nutzer nahtlos und geschieht vollständig im Hintergrund.

Hinweis: Wenn der Benutzer das Datenraum-Fenster im Browser neu lädt oder aktualisiert, muss er seinen Daten-Schlüssel (also das Passwort, das seinen privaten RSA-Schlüssel schützt) erneut eingeben. Das liegt daran, dass WebCrypto nach dem Neuladen oder Aktualisieren der Seite alle Reste der importierten – und damit momentan (lokal im Browser) verfügbarer – Schlüssel löscht und der Datenraum-Schlüssel neu erzeugt werden muss.

5. Benutzer einladen

Jeder Benutzer, der in ein netfiles Data Vault eingeladen wird, benötigt ein RSA-Schlüsselpaar in seinem Benutzerkonto. Das bedeutet, dass der Benutzer bereits einen persönlichen Daten-Schlüssel festgelegt hat. Entsprechend gibt es zwei Ablaufmöglichkeiten einer Einladung:

Benutzer besitzt ein RSA-Schlüsselpaar („Daten-Schlüssel“)

Wenn ein Benutzer eingeladen wird und bereits ein Schlüsselpaar aus privatem und öffentlichem RSA-Schlüssel besitzt, ist die Einladung nahtlos: Der Administrator gibt beim Betreten des Data Vault seinen persönlichen Daten-Schlüssel ein. Dadurch wird – lokal im Browser – der Datenraum-Schlüssel-Seed entschlüsselt und verfügbar gemacht. netfiles verschlüsselt diesen – ebenfalls lokal im Browser – mit dem öffentlichen RSA-Schlüssel der eingeladenen Person. Anschließend wird dieser neu verschlüsselte Datenraum-Schlüssel-Seed im Konto des eingeladenen Benutzers (für dieses Data Vault) gespeichert.

Nachdem der Benutzer die Einladung angenommen hat, muss er wiederum seinen persönlichen Daten-Schlüssel eingeben. Dadurch wird (lokal im Browser) der Datenraum-Schlüssel-Seed entschlüsselt, ein Datenraum-Schlüssel aus dem Datenraum-Schlüssel-Seed erzeugt und der Benutzer kann dem Data Vault direkt beitreten.

Benutzer besitzt noch kein RSA-Schlüsselpaar („Daten-Schlüssel“)

Wenn ein eingeladener Benutzer noch kein Schlüsselpaar aus privatem und öffentlichem RSA-Schlüssel besitzt, ist im Einladungs-Prozess eine zweite Bestätigung durch den Administrator erforderlich:

1. Der Administrator lädt den Benutzer in einen Datenraum ein. Bei Versand der Einladung darüber informiert, dass er einen Benutzer ohne RSA-Schlüsselpaar einlädt und daher eine zweite (endgültige) Bestätigung vornehmen muss, sobald der Benutzer die Einladung angenommen und ein Schlüsselpaar erstellt hat.

2. Wenn der eingeladene Benutzer die Einladung annimmt, fordert netfiles ihn auf, einen Daten-Schlüssel festzulegen und erzeugt ein RSA-Schlüsselpaar (der Ablauf erfolgt wie in Kapitel 4. Implementierung beschrieben).

3. Nachdem die Benutzer-Schlüssel erzeugt sind, teilt netfiles dem Administrator mit, dass der Benutzer bereit ist, den Datenraum zu betreten. Dem Benutzer teilt netfiles mit, dass eine zweite, endgültige Bestätigung durch den Administrator erforderlich und veranlasst worden ist. Der Benutzer wird per E-Mail informiert, sobald der Administrator die Bestätigung erteilt hat und der Zugriff auf den verschlüsselten Datenraum möglich ist.

4. Der Administrator wird per E-Mail darüber informiert, dass der eingeladene Benutzer nun ein RSA-Schlüsselpaar besitzt und auf seine endgültige Bestätigung wartet. Wenn der Administrator den Benutzer freigibt, führt netfiles den Prozess für Benutzer durch, die bereits ein RSA-Schlüsselpaar besitzen (wie oben beschrieben).

Übersicht: Freigabe eines netfiles Data Vault an eingeladenen Benutzer