

## LEISTUNGSBESCHREIBUNG

### 1. Definition

**RWT secure Datashare** ist eine Softwarelösung, um große Dateien einfach, verschlüsselt, sicher und nachvollziehbar mit Partnern auszutauschen und zu speichern. Alle dabei abgelegten Daten werden ausschließlich auf dem RWT internen Serversystem abgelegt. Nur zuvor berechnigte Nutzer können auf die Daten zugreifen.

**RWT secure Datashare** arbeitet browserbasiert, so dass weder zur Speicherung noch zum Versand oder Empfang neben einem Webbrowser und einer Internetverbindung zusätzliche Clientsoftware installiert werden muss.

**RWT secure Datashare** bietet zur sicheren Datenübertragung und Speicherung:

- die verschlüsselte Übertragung von Dateien und Textnachrichten sowie
- verschlüsselte Datenräume- und Speicher („**RWT secure Datashare**“).

### 1.2. RWT secure Datashare Datenräume

Über **RWT secure Datashare** Datenräume können Dateien ausgetauscht und gemeinsam bearbeitet werden.

Die im **RWT secure Datashare** abgelegten Daten sind immer verschlüsselt.

Es können Verzeichnisse und darin enthaltene Dateien zwischen dem Endgerät eines Nutzers und den **RWT secure Datashare** Datenraum ausgetauscht werden. Dateien, die durch zwei Nutzer gleichzeitig bearbeitet werden, werden nicht überschrieben, sondern versioniert abgelegt.

### 2. Leistungen

Folgend aufgeführte Leistungsmerkmale werden bereitgestellt:

Datenraum für 30/90/180 Tage	ja
Brute Force Protection (Sperrung nach 10 maligem Fehlversuch)	ja
Datensicherung	ja
Mail-Verschlüsselung (E-Mail Benachrichtigungen)	ja
Ende-zu-Ende-Verschlüsselung (Datenraum)	ja

Gemeinsames Bearbeiten von Dateien	ja
Reporting & Event Logs (nur IT intern)	ja

Im Folgenden werden die Leistungen beschrieben:

Leistungsmerkmal	Beschreibung
Datenraum	Die Verwendung des <b>RWT secure Datashare</b> dient lediglich zum Austausch von Dateien und Informationen für einen begrenzten Zeitraum. Bei der Anlage des Datenraums legt der jeweils zuständige RWT-Ansprechpartner die Nutzungsdauer von 30/90/180 Tagen fest. Nach Ablauf dieser Frist werden die Daten unwiderruflich gelöscht!
Max. Dateigröße	Die Dateigröße einer Datei ist auf 500 MB begrenzt. Maximal darf pro Mandant eine maximale Größe von einem Terrabyte (dies entspricht ca. 1000 GB) belegt werden.
Brute Force Protection	Wird eine Anzahl von Login-Fehlversuchen für einen <b>RWT secure Datashare</b> -Account erreicht (10 Versuche), muss die erneute Freischaltung beantragt werden. Damit können automatisierte Angriffe (Brute Force Angriffe) unterbunden werden.
Datensicherung	Zur Absicherung im Falle eines Systemausfalls sichert der Anbieter periodisch mit einem Intervall von einem (1) Tag die Systemdaten (d. h. nicht die Dateien und Textnachrichten des Kunden) zum Betrieb.
Verschlüsselte E-Mail Zustellung	Informationen über E-Mail werden auf dem Transportweg, bis sie beim Empfänger ankommen, dauerhaft per TLS verschlüsselt.
Ende-zu-Ende-Verschlüsselung (Datenräume)	<b>RWT secure Datashare</b> Datenräume sind grundsätzlich Ende-zu-Ende verschlüsselt. Die Daten werden auf dem Endgerät des Nutzers verschlüsselt und via HTTPS/SSL in dem <b>RWT secure Datashare</b> Datenraum abgelegt. Die Entschlüsselung erfolgt erst wieder beim Download der Datei auf dem Endgeräte des Nutzers.
Gemeinsames Bearbeiten von Dateien	<b>RWT secure Datashare</b> Nutzer können Dateien hoch und herunterladen. Arbeiten zwei Nutzer an selben Dokument, erkennt <b>RWT secure Datashare</b> beim Upload einen ggf. vorliegenden Versionskonflikt und legt die betreffende Datei automatisch als neue Version ab.
Reporting & Event Logs	Ereignisse, die in <b>RWT secure Datashare</b> durchgeführt werden, werden protokolliert. Damit stehen den RWT Administratoren Analysemöglichkeiten zur Nutzung und Optimierung des Systems zur Verfügung. Der Report stellt Anzahl der Versendungen, Größe der Versendungen, verwendeter Speicher und durchgeführte Aktionen dar.

### 3. SSL-Zertifikat

Zum Betrieb von **RWT secure Datashare** wird ein namhaftes offizielles 256bit SSL-Zertifikat verwendet.

### 4. Systemanforderungen, Mitwirkung des Kunden

Die dauerhafte Sicherstellung der im Folgenden beschriebenen Systemanforderungen liegt im Verantwortungsbereich des Kunden.

#### 4.1 Internetanbindung

Der Kunde ist für die Anbindung seiner Systeme an das Internet in ausreichender Bandbreite verantwortlich.

##### 4.1.1. Anpassung Firewall für Client-Anwendungen

Zum Betrieb von **RWT secure Datashare** ist eine IP-Verbindung von den Endgeräten über das Kunden-LAN zur Umgebung des Anbieters erforderlich. Da es sich um übliche PC-Internet-Kommunikation handelt, erfolgt diese in der Regel über eine Internet-Firewall des Kunden. Folgende Ports sind auf der Kunden Internet-Firewall zu öffnen:

Benötigte Port-Freischaltungen auf Kunden-Firewalls					
Port	Quelle	Ziel	Protokoll	Type	Verwendung
443	Client	Server	HTTPS	TCP	Server Requests

##### 4.1.2. Anforderungen an die Computerumgebung

Die eingesetzten Endgeräte des Kunden müssen die folgenden Systemvoraussetzungen erfüllen:

Komponente	Anforderung
Browser	<ul style="list-style-type: none"><li>• Alle gängigen Internet Browser</li></ul>
Office Paket	<ul style="list-style-type: none"><li>• Zur sinnvollen Nutzung wird ein Standard Office Paket empfohlen (z. B.: MS Office)</li></ul>