Storebox Security

Whitepaper

Stefan Lengacher

swisscom

Zusammenfassung für Entscheider

Swisscom Produkte enthalten die nötigen Funktionen damit die Daten der Kunden sicher verwaltet und gespeichert werden. Swisscom setzt dabei auf bewährte «Standard of Good Practice»-Security. Der Chief Security Officer von Swisscom rapportiert direkt an den CEO von Swisscom, um zu gewährleisten, dass die nötigen Security-Prozesse und Security-Funktionen umgesetzt werden. Mehrere hundert Mitarbeiter sind in verschiedensten Security-Funktionen tätig um die Sicherheit der Kundendaten zu gewährleisten. Swisscom ist nach ISO27001:2013 zertifiziert.

Die Swisscom Data Center für den Service Storebox erfüllen die höchsten Anforderungen betreffend Verfügbarkeit und Vertraulichkeit. Diese Massnahmen beinhalten die nötigen physischen Schutzmassnahmen wie Rund-um-die-Uhr-Loge mit Sicherheitspersonal, Videoüberwachung, Brandschutz, unterbrechungsfreie Stromversorgung sowie getrennte Material- und Personenzugänge. Auch die Data Center unterstehen der ISO27001:2013-Zertifizierung von Swisscom (Schweiz) AG.

Inhaltsverzeichnis

Die Komponenten von Storebox

Das Storebox Portal

Das Storebox Portal ist eine skalierende Plattform, welche das Erstellen, Bereitstellen und das Management von Cloud-Storage-Applikationen erlaubt. Diese beinhalten Lösungen wie File-Sharing und –Synchronisation, Backup und mobile Kollaboration. Sie wirken als Middleware, welche den Swisscom Storage (siehe nächstes Kapitel) mit den Storebox Clients / Endgeräten verbindet.

Die Portal-Infrastruktur (Server) wird zu 100% von Swisscom betrieben. Ein allfälliger externer Zugriff des Herstellers im Falle von Betriebsleistungen geschieht nur unter kontrollierter Aufsicht des Swisscom-Betriebspersonals.

Storebox Storage

Der Storebox Storage bezieht den Service von Swisscom Dynamic Storage. Dieser Objektspeicher, basierend auf EMC Atmos, ist unterteilt auf mehrere Storage-Nodes, welche über verschiedene Rechenzentren von Swisscom in der Schweiz verteilt liegen und steht somit hochredundant zur Verfügung. Daten, welche auf diesem Storage gespeichert sind, verlassen die Schweiz nie und der Betrieb dieser Infrastruktur liegt zu 100% bei Swisscom.

Storebox Client

Storebox Clients sind Software Clients, welche auf Workstations oder Servern installiert werden können. Dabei können diese im sogenannten «Local Mode», welcher hybride file-level und disk-level Backups via einem NAS-Gateway erlaubt, oder im sogenannten «Cloud Mode», welcher Filesynchronisation und – Share und Backup direkt ins Storebox-Portal erlaubt, betrieben werden.

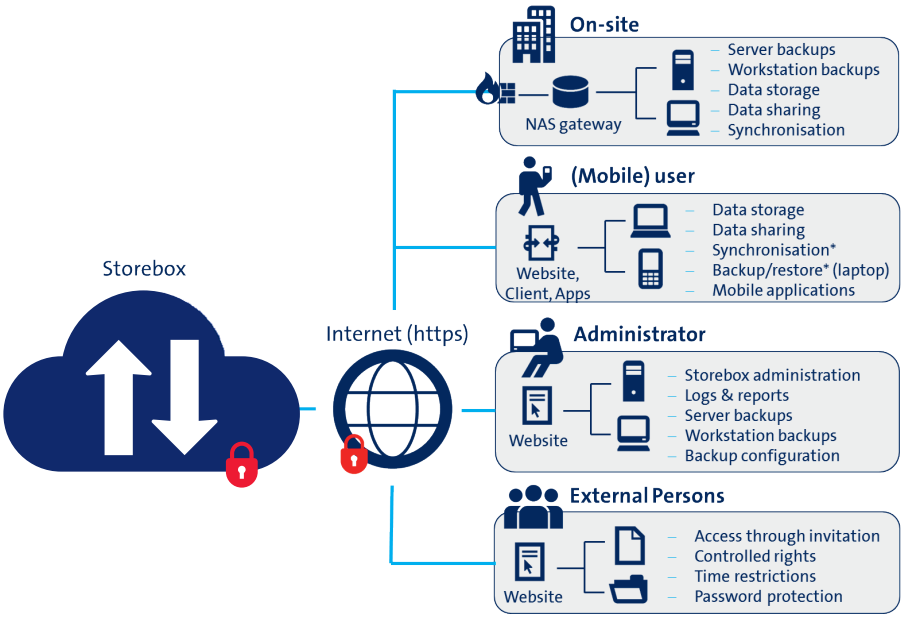
Storebox Mobile Apps

Die Storebox Mobile-Applikationen sind Smartphone-Applikationen, welche den sicheren Zugang zu den Daten im Storebox-Portal und die Kollaboration mittels dieser Daten mit externen Personen erlauben. Diese Mobile-Apps wurden durch Swisscom auf ihre Sicherheit geprüft. Neue Versionen testet Swisscom risikobasiert.

Storebox NAS-Gateways

Storebox NAS-Gateways sind Hardware-Appliances, welche vor Ort oder in entfernten Filialen oder Büros installiert werden können. Sie wirken als lokale, Cloud-integrierte Datenspeicher (NAS). Sie erlauben die Aggregation von Daten für mehrere Benutzer, das Synchronisieren dieser Daten und die optimierte Sicherung (Backup) und Wiederherstellung (Restore) mit dem Storebox-Portal.

Das folgende Diagramm beschreibt, wie diese Komponenten in der Gesamtlösung Storebox zusammenpassen:



Die Komponenten des Storebox Portals

Das Storebox Portal besteht aus folgenden Komponenten:

Hauptdatenbank

Das Storebox Portal nutzt eine Hauptdatenbank um sämtliche systemrelevanten Informationen wie User-Accounts, Storebox Clients etc. zu speichern. Diese Hauptdatenbank speichert sensitive Metadaten, wie z.B. Usernamen und Secret Keys. Nur der Applikationsserver hat Verbindung zu dieser Hochsicherheits-Zone, da dieser Datenbankserver in einem privaten Netzwerk ohne direkten Internet-Zugang sitzt. Dieser Datenbankserver fungiert auch als sogenannter «Catalog Node», welcher die objektrelevanten Informationen über die Dateien und Blocks der Backups beinhaltet.

Front-End Applikationsserver

Das Storebox Portal nutzt einen Web-Server um den Benutzern den Zugang zu ihrer Storebox via Web-Interface (im Browser) und via Mobile-Applikationen zu ermöglichen. Der Web-Server fungiert dabei auch als Endpunkt der Kommunikation mit den Storebox Clients. Der Applikationsserver kommuniziert nur über verschlüsselte Verbindungen (HTTPS und TLS Verbindungen) mittels AES (Advanced Encryption Standard) und authentisiert mittels einem 2048 bit RSA X.509 Zertifikat. Zwecks Verfügbarkeit und Load-Balancing sind mindestens 2 solche Server in Betrieb bei Swisscom. Diese sind in einer sogenannten DMZ (Demilitarized Zone) untergebracht und werden durch einen «Application Delivery Controller» (ADC) und einem IDS/IPS System geschützt und überwacht.

Storage Infrastruktur

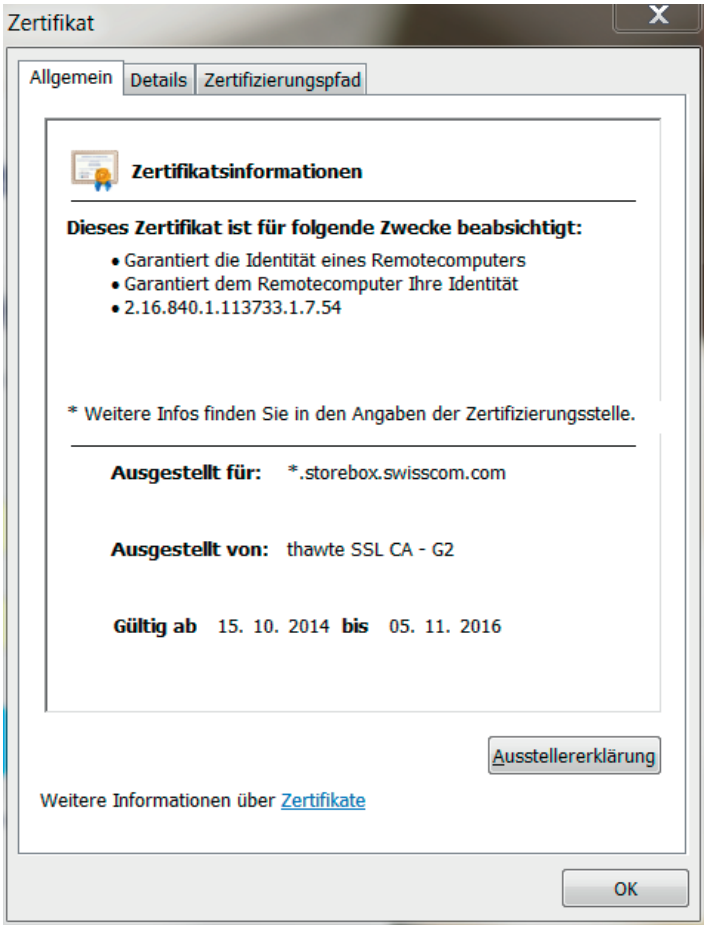
Sämtliche gespeicherten Daten (data at rest) auf den Storage Nodes werden mittels symmetrischem AES-256 verschlüsselt. Dieser Verschlüsselungsmechanismus wird auf den gesamten Storebox Storage angewandt (Backup-Verzeichnisse und «Cloud Drive»-Ablagen). Es werden in keiner Art und Weise Klartextdaten auf dem Storage-System abgelegt. Selbst für den unwahrscheinlichen Fall, dass ein Angreifer Lese-Zugriff auf das Storage-System erhalten sollte, kann er den Inhalt der Daten nicht einsehen.

Um vor bösartiger Verfälschung oder Korruption durch Personen mit Zugriff auf die Storage- Infrastruktur zu schützen, wird jede einzelne Datei mittels HMAC-SHA-1 signiert. Zusätzlich schützt ein MD5-Hash jeden individuellen Datenblock vor Korruption. Dies dient zudem als zusätzlicher Integritäts-Check, der auch ohne den Verschlüsselungs-Schlüssel angewandt werden kann.

Die Security Features

Das Storebox Portal X.509 Zertifikat

Das Storebox Portal nutzt ein 2048-bit X.509 Sicherheitszertifikat um Web-Browser, NAS-Gateways und Storebox Clients gegenüber dem Storebox Portal zu authentisieren. NAS-Gateways und Storebox Clients nutzen hierfür TLS-Verbindungen, während die Web-Browser HTTPS nutzen.



Die Mandantenfähigkeit des Storebox Portals

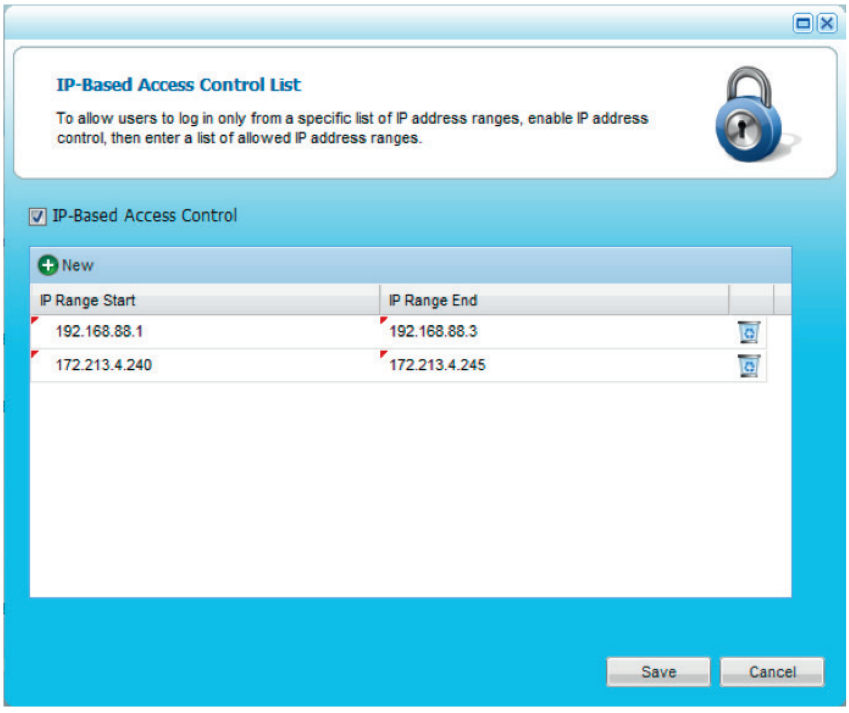
Mandantenfähigkeit bedeutet, dass mit einer einzelnen Instanz von Software mehrere Kunden, sogenannte «Tenants», verwaltet werden können. Die Mandantenfähigkeit des Storebox Portals erlaubt das Delegieren von diversen Service-Delivery-Aspekten zu Kunden und Partnern, indem virtuelle Portal-Instanzen (Tenants) des Storebox Portals verwendet werden. Jedes dieser virtuellen Portale ist komplett isoliert von den anderen Instanzen. Das Storebox Portal unterstützt virtuelle Portal-Instanzen (Tenants), welche «Teamportal» genannt werden. Benutzerkonten von verschiedenen solchen Instanzen sind komplett separiert, ebenso deren gesicherten Daten.

Storebox Portal Zugriffskontrolle

Das Storebox Portal unterstützt 2 Methoden, um die Zugriffe zu begrenzen:

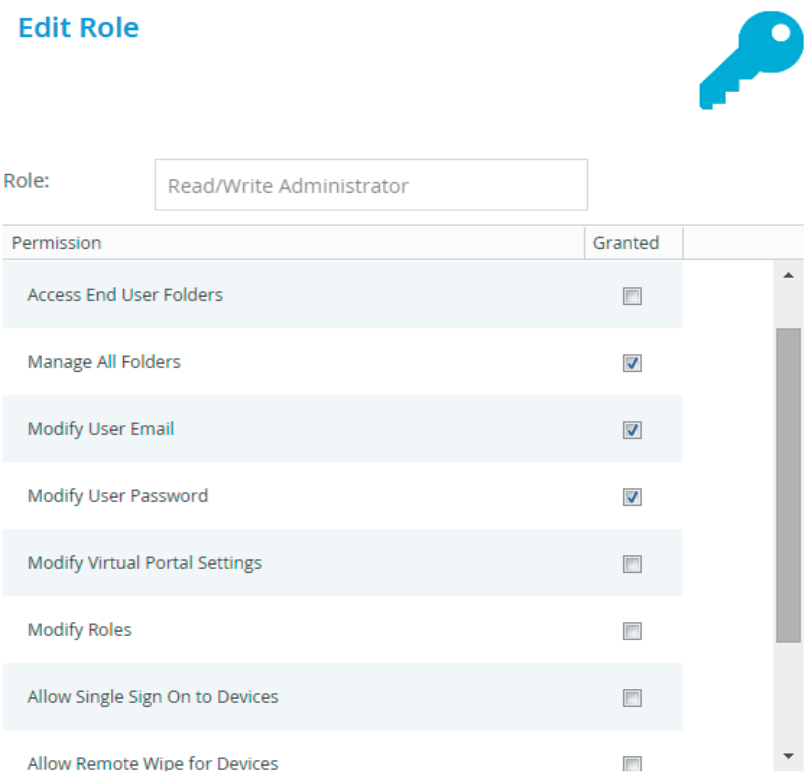
1. IP-Based Access Control (nur verfügbar bei dedizierter Storebox)

Es ist möglich, eine Liste von spezifischen IP-Adressbereichen zu definieren, von wo aus sich Administratoren auf das Portal einwählen dürfen.



2. Rollenbasierte Zugriffskontrolle

Jedem Benutzerkonto im Storebox Portal wird eine Rolle zugewiesen, welche den Autorisierungsgrad im System definiert. Gleichermassen wird jedem Administrator eine entsprechende Rolle zugeteilt (z.B. Read/Write vs. Read-only). Es ist zudem möglich, die einzelnen Berechtigungen selber zu definieren. Unabhängig ihrer Rolle können Administratoren sich nicht einfach als Benutzer einwählen oder irgendwelche Aktionen ausführen, welche einem Benutzer zugeordnet würden. Der Storebox Service ist so konfiguriert, dass Storebox Administratoren standardmässig nicht auf Benutzerdaten zugreifen können. Sämtliche Administrator-Aktionen sind beschränkt auf die rollenbasierte Definition und werden (zusammen mit der Identität des Administrators) komplett im Audit-Log protokolliert.



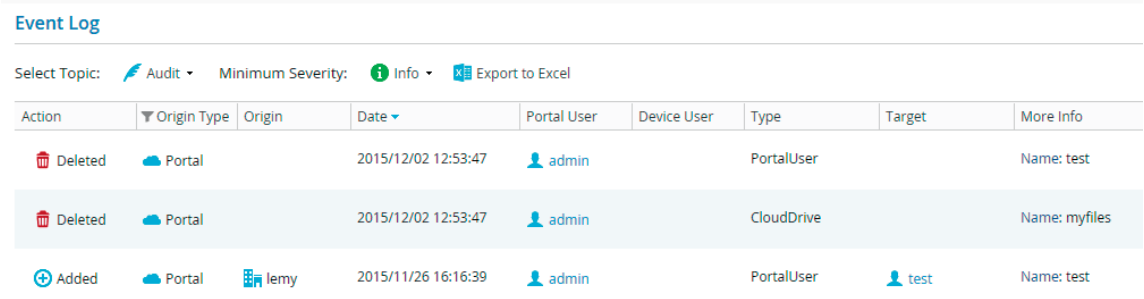
CTERA Transport Protocol

Für maximale Sicherheit der Lese- und Schreiboperationen zwischen den Storebox Clients und dem Storebox Portal wurde ein hocheffizientes, WAN-optimiertes Datei-Transfer-Protokoll, das CTERA Transport Protocol (CTTP) entwickelt. CTTP ist ein TCP-basiertes Protokoll, welches die Kommunikation «in transit» via dem Industriestandard TLS mit einer konfigurierbaren Chiffre (Standardmässig AES-256) verschlüsselt. «Backup», «Restore» und Synchronisation werden mittels CTTP über den TCP-Port 995 wie folgt übermittelt:

1. Wie bereits erwähnt, nutzt das Storebox Portal ein 2048-bit X.509 Zertifikat, welches die Verbindungen der Storebox Clients und Web Browser mit dem Portal authentisiert.
2. Für die initiale Registrierung, stellt der Storebox Client eine Verbindung mit dem Portal mittels Benutzername und Passwort-Authentisierung her. Danach erhält dieser einen einmaligen 256-bit Authentisierungsschlüssel, welcher für sämtliche späteren Verbindungen anstelle des Benutzername-Passwort-Paares verwendet wird.
3. Vor der Übertragung verschlüsselt der Storebox Client alle Dateifragmente mittels AES-256 CBC.
4. Die hierfür benötigten Schlüssel werden nie dauerhaft im Client gespeichert. Das Storebox Portal dient dabei als Schlüssel-Server (Key Server) und stellt den Data Encryption Key (DEK) Schlüssel dem Client zur Verfügung, sobald dieser Zugang zu einem Cloud-Ordner beansprucht.
5. Für die Backup-Funktion kann im Storebox Client zusätzlich ein individuelles Passwort erstellt werden. Aus diesem Passwort leitet der Storebox Client den sogenannten «Key Encryption Key» (KEK) mittels des PBKDF2 Key Derivation Algorithmus her. Bei den NAS-Gateways wird der KEK dauerhaft im Flash Memory gespeichert.
6. Das Storebox Portal erhält weder den KEK noch den DEK. Stattdessen wird der KEK benutzt, um den DEK mittels AES-256 «Key Wrapping» Algorithmus (wie in RFC-3394 definiert) zu verschlüsseln. Das entstandene Resultat wird im Storebox Portal als «Encrypted Folder Key» (EFK) abgelegt.
7. Um die Backup-Daten zu entschlüsseln erfragt der Storebox Client als erstes den EFK vom Storebox Portal für einen spezifischen Ordner.
8. Das Storebox Portal überprüft zuerst, ob dieser Storebox Client die benötigte Berechtigung für den Zugriff auf diesen Ordner hat und retourniert den EFK wenn dem so ist.
9. Schliesslich decodiert der Storebox Client den EFK mittels dem KEK um den DEK zu erhalten. Diesen nutzt er dann, um die Daten erfolgreich im Ordner zu sichern (Backup) oder wiederherzustellen (Restore).

Storebox Audit Log

Sowohl das Storebox Portal als auch die Storebox NAS-Gateway Web-Interfaces stellen ein ausführliches Protokoll aller Konfigurations- und Datenänderungen zur Verfügung. Eine der Protokollarten ist das sogenannte «Audit Log», welches die verschiedenen Konfigurations-Änderungen (typischerweise durch Administratoren durchgeführt) protokolliert. «Audit Logs» beinhalten Informationen zur Art der Änderung, den Account-Namen, das Datum, einen Zeitstempel, das beeinflusste Element etc. Das Storebox Portal kann auch sämtliche Datenänderungen und Datenzugriffe protokollieren.



Im Storebox Portal ist das Audit Log verfügbar für den/die Storebox Administator(en).

Eine dedizierte Storebox erlaubt zudem das Weiterleiten der Protokolle an einen eigenen Syslog Server für weiterführende Analysen und vieles mehr.

Storebox Portal - zusätzliche Sicherheit

Das Storebox Portal nutzt «best practices» um seine Daten zu schützen: So werden automatisch sogenannte «buffer overruns» überprüft und erkannt und das System beinhaltet HTML- Verifizierungstechnologien, welche Cross-Site-Scripting-Attacken (XSS) abwehrt und spezifische Überprüfungen durchführt, um potentielle Attacken wie z.B. Cross-Site Request Forgery (CSRF), XEE, ClickJacking etc. zu erkennen und abzuwehren.

Die Storebox Umgebungen sind sogenannte «hardened virtual appliances». Nur minimalste Konfigurationen (wie IP Addresse etc.) werden auf dessen File System gespeichert und der Zugang zu diesen Daten ist mittels SSH-Passwort und -Zertifikat geschützt. Der Rest der Konfiguration ist in der Hauptdatenbank gespeichert und durch entsprechende Sicherheitsmechanismen geschützt. Konfigurationsänderungen werden im Storebox Audit Log zusammen mit dem ausführenden Usernamen protokolliert.

Alle Zugriffe (ob erfolgreich oder nicht) werden protokolliert. Zusätzlich bietet das System die Möglichkeit, dem Administrator auf Protokolleinträgen basierende Email-Alerts zu senden. Wenn ein Storebox-Client 3 mal erfolglos einzuwählen versucht, weil ein falsches Username/Passwort Paar verwendet wurde, werden sämtliche Login-Versuche von dieser Adresse für 5 Minuten gesperrt. Dieser Mechanismus minimiert drastisch die Gefahr von sogenannten «Password Guessing Attacks».

Session Management

Das Session Management bei Storebox fokussiert auf das Verhindern von Session Prediction, Capture und Hijacking. Session Prediction meint das Erraten von gültigen Session Identifiers. Mit dem Storebox Portal können Session Identifiers nicht erraten werden, weil die Session ID mittels einem sicheren Zufallsnummern-Generator erzeugt wird. Session Capture wird unterbunden, indem nur verschlüsselte Kommunikationskanäle verwendet werden (das Storebox Portal sendet die Session ID niemals mittels Klartextprotokollen). Session Hijacking wird unterbunden indem ein spezieller «CSRF Protector Header» verwendet wird und indem der Session Identifier bei jedem Login geändert wird. Dies unterbindet auch «Session Fixation Attacks». Wenn ein Benutzer 30 Minuten inaktiv ist, wird dieser automatisch ausgeloggt.

Storebox NAS-Gateway Sicherheit

Das Storebox NAS-Gateway basiert auf einer minimalen, sicherheitsgehärteten Version von Linux, in welchem virtuell sämtliche Standardservices ausgeschaltet sind, um potentielle Angriffsziele zu verhindern.

Das Storebox NAS-Gateway unterstützt das Erstellen von verschlüsselten Volumes. Wenn ein Administrator die Verschlüsselung des Inhalts eines Volumes aktiviert, muss er ein Passwort eingeben. «Password-Based Key Derivation Function 2» (PBKDF2) wird verwendet, um dieses zusätzlich zu sichern. Das Passwort wird anschliessend verwendet um den Verschlüsselungsschlüssel mittels AES-256 zu verschlüsseln. «Volume Encryption» basiert auf «Linux Unified Key Setup (LUKS). Diese Methode ist auf dem «TKS1 Key Setup»-Schema aufgebaut.

Zwei-Faktor-Authentifizierung

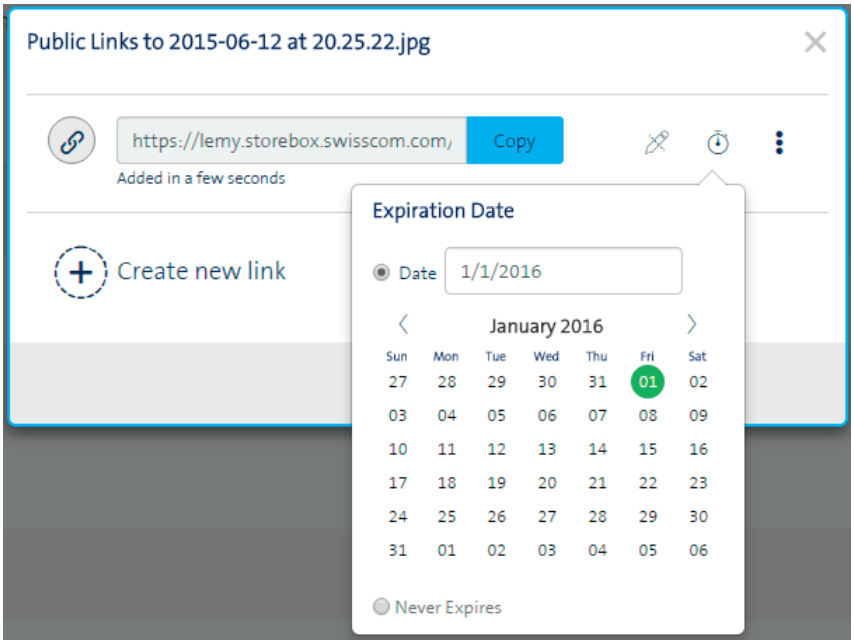
Storebox unterstützt die Zusammenarbeit an Daten, indem die Nutzer Gäste via Public Link einladen können. Diese Einladungen sind zeitlich limitierte URLs, welche einen Sicherheitscode beinhalten. Sie erlauben es dem Gast, den Inhalt eines Ordners oder einer Datei einzusehen oder diesen zu ändern.

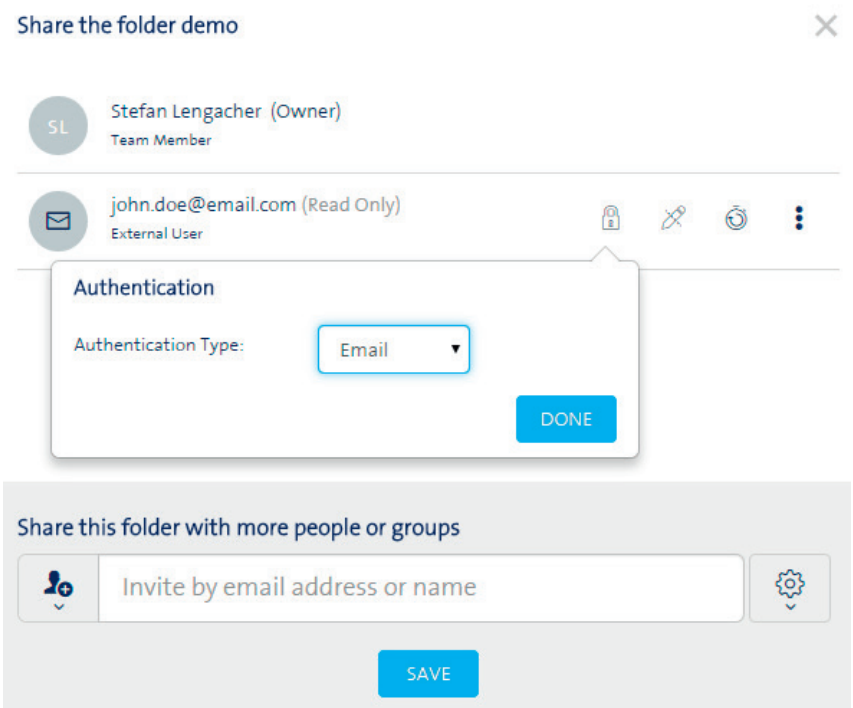
Der Storebox Administrator kann dabei selber definieren, welche Benutzer die Berechtigung haben, solche Einladungen zu erstellen und zu versenden (dies ist pro Benutzer oder pro Benutzergruppe möglich).

Storebox erlaubt eine Zwei-Faktor-Authentifizierung für solche Einladungen, basierend auf zufälligen Nummern-Codes (6-stellig), resp. »Challenges". Diese werden E-Mail an den eingeladenen Gast versandt, sobald er die URL in einem Browser öffnet. Diese Eigenschaft schützt davor, dass Einladungen weitergeleitet werden resp. von Dritten unerwünscht aufgerufen werden können. Die Zwei-Faktor-Authentifizierung ist gegen «Brute Force»-Attacken geschützt: Wird der Code fünf Mal falsch eingegeben, verliert dieser automatisch seine Gültigkeit. Zusätzlich werden sogenannte «Rate Limits» angewandt, um die Anzahl Authentifizierungsanfragen zu limitieren und «Denial of Service»-Attacken zu unterbinden.

Nach erfolgreicher Zwei-Faktor-Authentifizierung auf privaten Computern, erhält der User die Option, seinen Computer als «Trusted» zu definieren. Wählt er diese Option, wird ein zufälliger, eindeutiger 256-bit-Schlüssel auf diesem Gerät gespeichert. Während den nächsten 30 Tagen muss für den Zugriff (via Public Link) von diesem Gerät aus kein Code mehr eingegeben werden.

Sämtliche Zugriffe via Public Link, ob erfolgreich oder nicht, werden im Storebox Portal protokolliert.





Zugriffe der Lieferanten

Swisscom bietet Storebox in Kombination aus verschiedenen Leistungen von Lieferanten von Swisscom an. Keiner der Lieferanten hat Zugriff auf produktive Systeme von Swisscom und die darin enthaltenen Daten. Deren Zugriffsmöglichkeiten beschränken sich strikt auf die Entwicklungs- und Test-Systeme um dort Fehler nachzuvollziehen oder Software Fixes einzuspielen. Sämtliche derartigen Zugriffe werden zeitlich limitiert und von Swisscom Mitarbeitenden kontrolliert.