A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

SecureFS

Schlüsselmanagement / Tools

Inhaltsverzeichnis

Autor	Anmerkung	Datum	Status
Thomas Frühbeck	Arbeitsversion	13.02.2012	DRAFT

A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

1. Einleitung

Dieses Dokument beschreibt die Management-Applikation des SecureFS Virtual Appliance Clusters

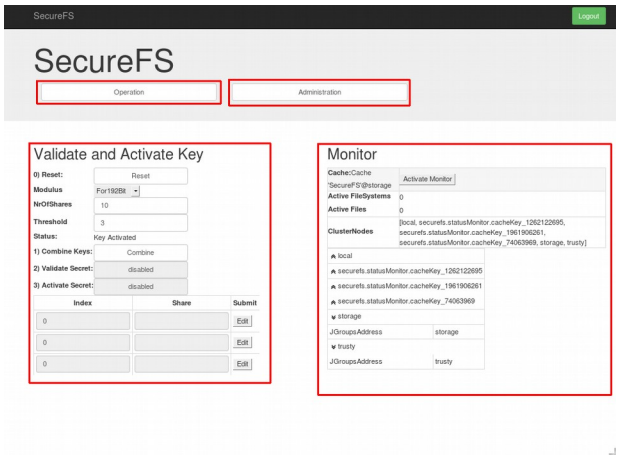
1.1. Rollen

Die Applikation kennt folgende Rollen:

- Administrator
  - Widerruf von Shares des aktuellen Schlüssels
  - Herstellung von Shares aus einem Geheimnis
  - Aktivierung eines neuen Schlüssels aus Shares – Datenverlust!!
  - Kopie von Dateihierarchien auf ein neues Verzeichnis, verschlüsselt mit einem evtl. neuen Schlüssel
- Operator
  - Aktivierung des aktuellen Schlüssels des Clusters – Prüfung der Korrektheit vor Aktivierung
  - Monitoring des Cluster-Zustands
- User
  - Lesen / Schreiben über die Schnittstellen der Virtual Appliance

1.2. Funktionsteile

Die Applikation bietet Funktionen für Operation und Administration, gemäß den Rollen.



1.2.1. Operation

Die Applikation bietet folgende Betriebs-Funktionen:

- Validate and Activate Key: kontrollierte Aktivierung des Schlüssels mittels Eingabe der benötigten Shares
- Monitor: Anzeige der im Cluster registrierten Virtual Appliances und der VA-lokalen Zustäne (zB Verfügbarkeit des Cluster-Schlüssels)

1.2.2. Management

Die Applikation bietet folgende Management-Funktionen:

- Widerruf von Shares des aktuellen Schlüssels
- Herstellung von Shares aus einem Geheimnis
- Aktivierung eines neuen Schlüssels aus Shares – Datenverlust!!
- Kopie von Dateihierarchien auf ein neues Verzeichnis, verschlüsselt mit einem evtl. neuen Schlüssel

A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

2. Operation

2.1. Aktivierung des aktuellen Schlüssels durch Shares

Der SecureFS-Cluster kennt im Betrieb einen aktiven Schlüssel, der für Schreib/Lesevorgänge genutzt wird.

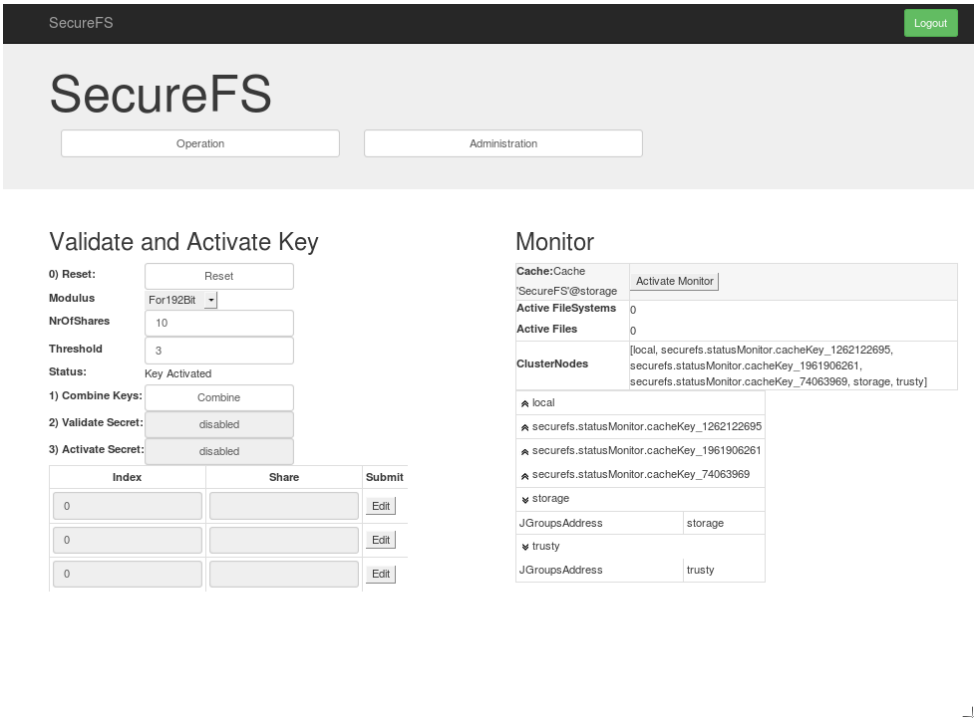
Dieser Schlüssel muss initial bei Inbetriebnahme des Clusters aktiviert werden. Die Aktivierung erfolgt durch potentiell räumlich und zeitlich unabhängige Eingabe der benötigen Shares (gemäß Erstellungsparameter des Schlüssels).

Während der Eingabe der Shares ist der aktuelle Share nur für den Benutzer der aktiven Browser-Session sichtbar, für die anderen Teilnehmer / Benutzer ist der Share anonymisiert.

2.1.1. Eingabe der Schlüssel-Parameter

Zuallererst müssen die korrekten Schlüssel-Parameter eingegeben werden:

- Modulus (Auswahl aus 3 vordefinierten Werten)
- NrOfShares: die Gesamtzahl der Shares, die bei der Erstellung des Schlüssels definiert wurden
- Threshold: Anzahl der benötigten Shares, , die bei der Erstellung des Schlüssels definiert wurden (siehe Konzept SecureFS, Shamir Key-Sharing)

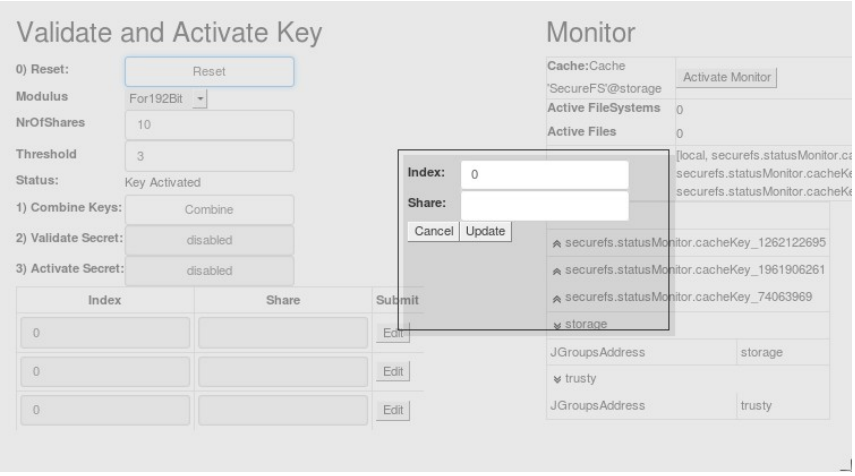


A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

2.1.2. Eingabe der Shares – Cluster-Remote

Nach Eingabe des Threshold-Wertes werden die benötigten Eingabefelder für die Shares angeboten und stehen zur Eingabe zur Verfügung.

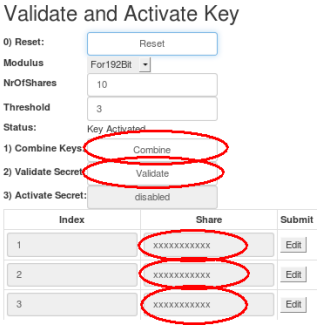
Jeder teilnehmende Operator/Administrator kann einen Share eingeben, die Eingabe selbst ist nur am aktiven lokalen Desktop sichtbar.



2.1.3. Validierung und Aktivierung des Schlüssels

Nach Eingabe der geforderten Shares werden die Shares zu einem Schlüssel umgewandelt (Combine), und der generierte Schlüssel kann validiert werden (Validate).

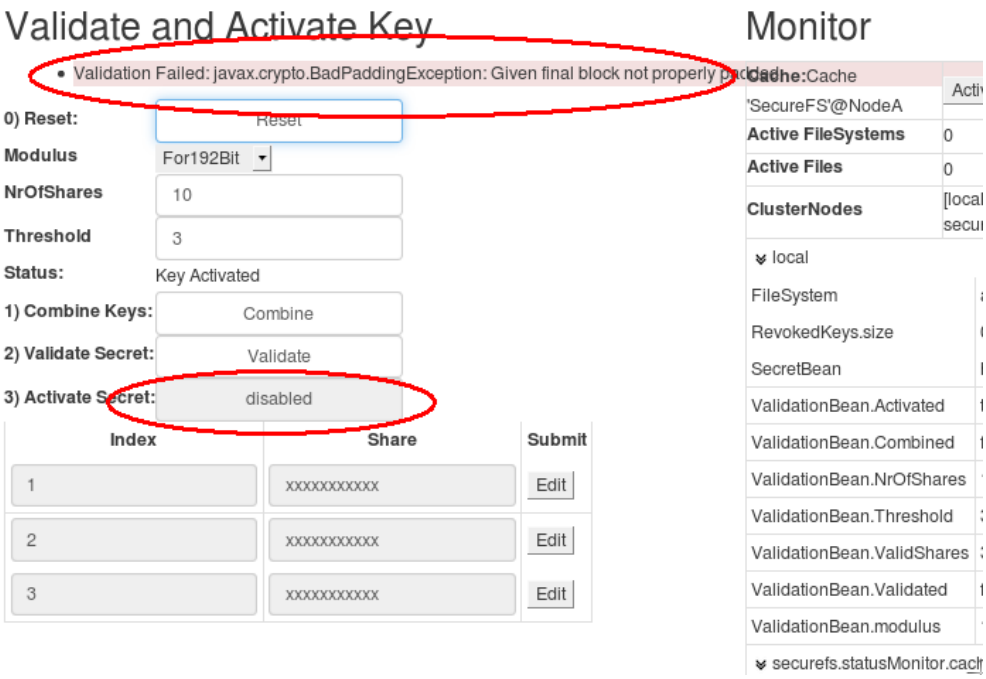
Die Validierung erfolgt über das Revocation-File des Clusters im Filesystem, wenn das File manipuliert / gelöscht wurde, kann die Validierung nicht erfolgen.



A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

2.1.4. Fehler bei Validierung (zB Eingabefehler)

Wenn ein Parameter der Schlüsselerstellung bzw. ein Share nicht korrekt eingegeben wurde, wird bei der Validierung eine Fehlermeldung erzeugt, und die Aktivierung dieses – sichtlich falschen – Schlüssels verhindert.



2.1.5. Verlust des Revocation-Files

Wenn es zu einem Verlust oder der Manipulation des Revocation-Files kommt, kann der Schlüssel über die Funktion Administration/Activate New Key hergestellt werde, dann kann allerdings keine Validierung erfolgen, und während der Verfügbarkeit dieses falschen Schlüssels Dateien unlesbar sein, bzw. Dateien mit falschem Schlüssel geschrieben werden.

A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

3. Administration

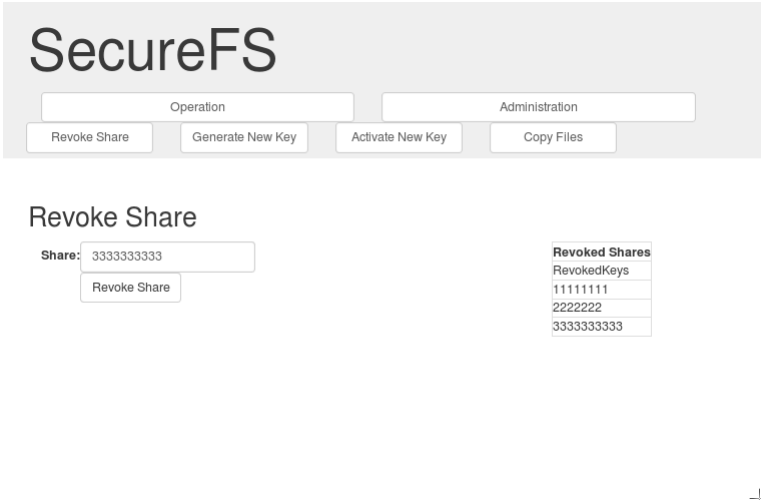
Die Funktionen der Administration stehen nur der Rolle Adminstrator zur Verfügung.

3.1. Widerruf eines Shares

Das System liest bei jedem Start das aktuelle Revocation-File, bei gewissen Operationen, und beim geordneten Shutddown wird das File neu geschrieben. Im laufenden regulären Betrieb ist also ein Verlust des Files unwahrscheinlich.

In der Funktion werden die akutell widerrufenen Shares angezeigt und eine Eingabe weiterer Shares angeboten.

Ein einmal widerrufener Share kann nicht wieder aktiviert werden, außer durch Zerstörung des Revocation-Files außerhalb des Betriebs des SecureFS-Clusters – Betriebsstörung.



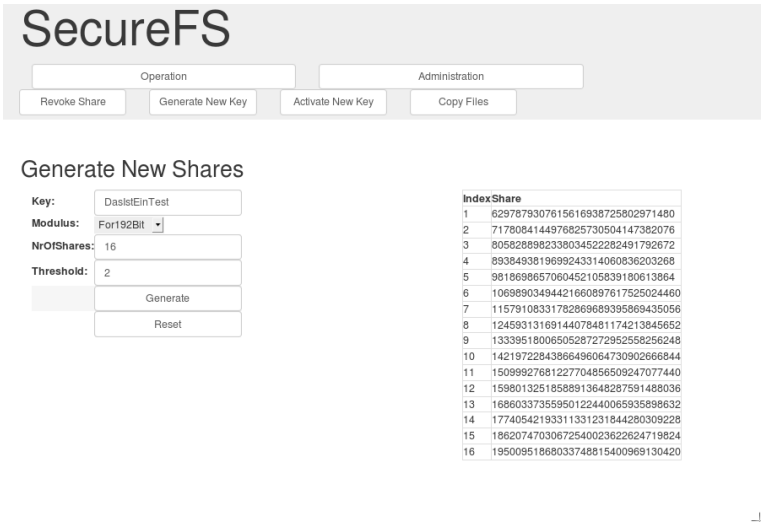
3.2. Generierung von Shares aus einem Geheimnis

Diese Funktion ermöglicht die Herstellung eines neuen Sets an Shares zur Herstellung eines Schlüssels.

Die Parameter sind:

- Key: das Geheimnis, aus dem der Schlüssel generiert werden soll
- Modulus: (Auswahl aus 3 vordefinierten Werten)
- NrOfShares: die Gesamtzahl der Shares, die bei der Erstellung des Schlüssels definiert wurden
- Threshold: Anzahl der benötigten Shares, , die bei der Erstellung des Schlüssels definiert wurden (siehe Konzept SecureFS, Shamir Key-Sharing)

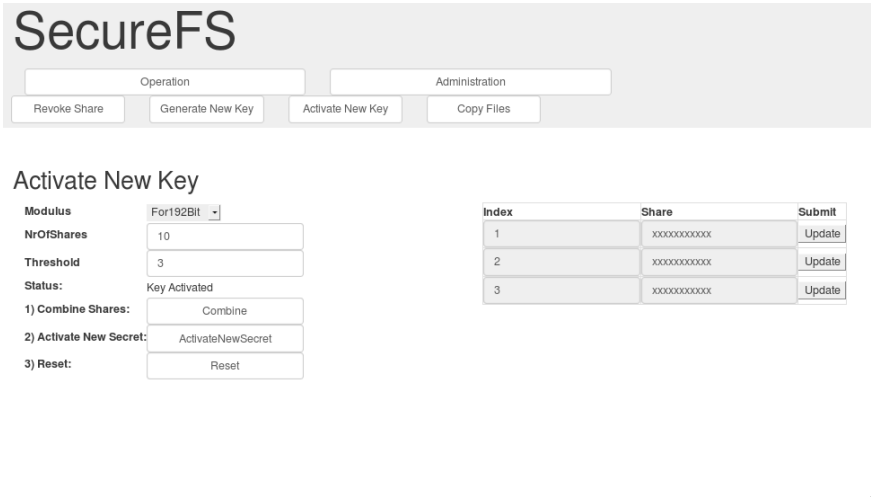
A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien



3.3. Aktivierung eines neuen Schlüssels

Parameter und Funktion analog zur Funktion Operator/Validierung und Aktivierung, allerdings erfolgt hier keine Validierung, eine Fehleingabe erzeugt einen falschen Schlüssel, die bereits existierenden Dateien können nicht gelesen werden.

Neu geschriebenen Dateien werden mit dem neuen Schlüssel verschlüsselt, der potentiell nicht wieder herstellbar ist (siehe Fehleingabe).



3.4. Kopieren einer File-Hierarchie auf neuen Schlüssel

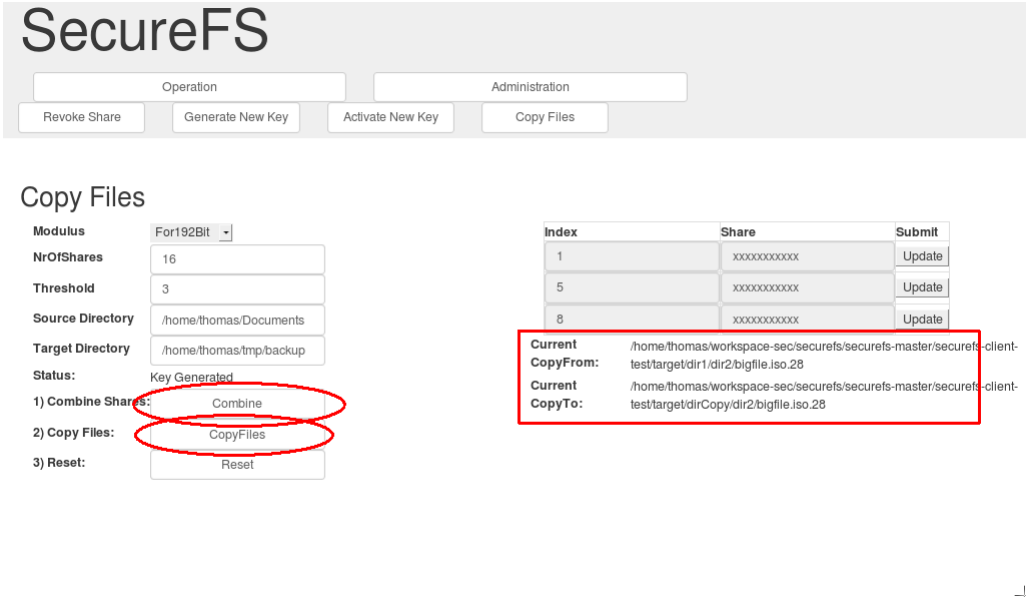
Diese Funktion ermöglicht die Übertragung von Datei-Hierarchien des aktuellen Clusters in ein neues Filesystem.

A1 Telekom Austria AG
ITS / SDE / B2B
Antonigasse
A-1170 Wien

Für die Verschlüsselung im Ziel-Filesystem kann ein neuer Schlüssel hergestellt werden. Vorgangsweise analog zu Activate New Key, allerdings wird der generierte Ziel-Schlüssel nicht zur Laufzeit in den Cluster publiziert, somit kann die Kopie parallel zum regulären Betrieb stattfinden.

Folgende Voraussetzungen müssen gelten:

- ein Schlüssel muss mittels Parameter und Shares (Combine) hergestellt sein
- das Quell-Filesystem muss lesbar sein
- der Startpunkt des Quell-Filesystems muss ein Verzeichnis sein
- das Ziel-Filesystem muss ein Verzeichnis sein
- das Ziel-Verzeichnis muss schreibbar sein
- das Ziel-Verzeichnis muss LEER sein, damit Datenverlust bei Fehlbedienung ausgeschlossen ist



3.4.1. Copy Files - Monitoring

Der Prozess des Kopiervorgangs kann im Monitoring mitverfolgt werden, es wird das aktuell bearbeitet File angezeigt, mit Quell- und Zielpfad.