

SecureFS

Schlüsselmanagement / Tools

Inhaltsverzeichnis

1. Einleitung	3
1.1. Rollen.....	3
1.2. Funktionsteile.....	3
1.2.1. Operation.....	4
1.2.2. Management.....	4
2. Operation	5
2.1. Aktivierung des aktuellen Schlüssels durch Shares.....	5
2.1.1. Eingabe der Schlüssel-Parameter.....	5
2.1.2. Eingabe der Shares – Cluster-Remote.....	6
2.1.3. Validierung und Aktivierung des Schlüssels.....	6
2.1.4. Fehler bei Validierung (zB Eingabefehler).....	7
2.1.5. Verlust des Revocation-Files.....	7
3. Administration	8
3.1. Widerruf eines Shares.....	8
3.2. Generierung von Shares aus einem Geheimnis.....	8
3.3. Aktivierung eines neuen Schlüssels.....	9
3.4. Kopieren einer File-Hierarchie auf neuen Schlüssel.....	9
3.4.1. Copy Files - Monitoring.....	10

Autor	Anmerkung	Datum	Status
Thomas Frühbeck	Arbeitsversion	13.02.2012	DRAFT

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.

The screenshot shows the SecureFS web interface. At the top, there is a 'SecureFS' header with a 'Logout' button. Below the header, there are two tabs: 'Operation' and 'Administration'. The 'Operation' tab is selected, showing the 'Validate and Activate Key' form. This form includes fields for 'Reset', 'Modulus', 'NrOfShares', 'Threshold', 'Status', and 'Key Activated'. It also has buttons for 'Combine Keys', 'Validate Secret', and 'Activate Secret'. At the bottom of the form, there is a table with columns 'Index', 'Share', and 'Submit'. The 'Administration' tab is also visible, showing the 'Monitor' section. This section includes a 'Cache/Cache' table with columns 'SecureFS@storage', 'Active Filesystems', and 'Active Files'. It also has a 'ClusterNodes' section with a table showing the status of various nodes.

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 Zustände (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

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 benötigten 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)

SecureFS

Logout

SecureFS

OperationAdministration

Validate and Activate Key

0) Reset:

Reset

Modulus

For192Bit

NrOfShares

10

Threshold

3

Status:

Key Activated

1) Combine Keys:

Combine

2) Validate Secret:

disabled

3) Activate Secret:

disabled

Index	Share	Submit
0		Edit
0		Edit
0		Edit

Monitor

Cache:Cache

SecureFS@storage

Activate Monitor

Active FileSystems

0

Active Files

0

ClusterNodes

[local, securefs.statusMonitor.cacheKey_1262122695, securefs.statusMonitor.cacheKey_1961906261, securefs.statusMonitor.cacheKey_74063969, storage, trusty]

local

securefs.statusMonitor.cacheKey_1262122695

securefs.statusMonitor.cacheKey_1961906261

securefs.statusMonitor.cacheKey_74063969

storage

trusty

JGroupsAddress

storage

JGroupsAddress

trusty

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.

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.

Validate and Activate Key

- Validation Failed: javax.crypto.BadPaddingException: Given final block not properly padded

0) Reset:

Modulus: For192Bit

NrOfShares:

Threshold:

Status: Key Activated

1) Combine Keys:

2) Validate Secret:

3) Activate Secret:

Index	Share	Submit
1	xxxxxxxxxx	<input type="button" value="Edit"/>
2	xxxxxxxxxx	<input type="button" value="Edit"/>
3	xxxxxxxxxx	<input type="button" value="Edit"/>

Monitor

Cache:Cache

SecureFS'@NodeA

Active FileSystems: 0

Active Files: 0

ClusterNodes: [local, securi]

local

FileSystem: ;

RevokedKeys.size: ;

SecretBean: ;

ValidationBean.Activated: ;

ValidationBean.Combined: ;

ValidationBean.NrOfShares: ;

ValidationBean.Threshold: ;

ValidationBean.ValidShares: ;

ValidationBean.Validated: ;

ValidationBean.modulus: ;

securefs.statusMonitor.cacfr

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 werden, dann kann allerdings keine Validierung erfolgen, und während der Verfügbarkeit dieses falschen Schlüssels Dateien unlesbar sein, bzw. Dateien mit falschem Schlüssel geschrieben werden.

3. Administration

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

3.1. Widerruf eines Shares

Das System liest bei jedem Start das aktuelle Revocation-File, bei gewissen Operationen, und beim geordneten Shutdown 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.

The screenshot shows the 'SecureFS' administration interface. At the top, there are two tabs: 'Operation' and 'Administration'. Under 'Operation', there are buttons for 'Revoke Share', 'Generate New Key', and 'Activate New Key'. Under 'Administration', there is a button for 'Copy Files'. Below the tabs, the 'Revoke Share' section is active. It features a text input field labeled 'Share:' containing the value '3333333333', and a 'Revoke Share' button. To the right, there is a table titled 'Revoked Shares' with the following content:

RevokedKeys
11111111
22222222
3333333333

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)

SecureFS

Operation

Administration

Revoke Share

Generate New Key

Activate New Key

Copy Files

Generate New Shares

Key:

Modulus:

NrOfShares:

Threshold:

Generate

Reset

IndexShare

1	6297879307615616938725802971480
2	7178064144976825730504147382076
3	805828898233803452282491792672
4	8938493819699243314060836203268
5	9818698657060452105839180613864
6	10698903494421660897617525024460
7	1157910833178286989395869435056
8	12459313169144078481174213845652
9	13339518006505287272952558256248
10	14219722843866496064730902666844
11	15099927681227704856509247077440
12	15980132518588913648287591488036
13	16860337355950122440065935898632
14	17740542193311331231844280309228
15	18620747030672540023622624719824
16	19500951868033748815400969130420

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).

SecureFS

Operation

Administration

Revoke Share

Generate New Key

Activate New Key

Copy Files

Activate New Key

Modulus:

NrOfShares:

Threshold:

Status:

1) Combine Shares:

2) Activate New Secret:

3) Reset:

Index	Share	Submit
1	xxxxxxxxxxxx	<input type="button" value="Update"/>
2	xxxxxxxxxxxx	<input type="button" value="Update"/>
3	xxxxxxxxxxxx	<input type="button" value="Update"/>

3.4. Kopieren einer File-Hierarchie auf neuen Schlüssel

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

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

The screenshot shows the SecureFS web interface. At the top, there's a header with the 'SecureFS' logo and two tabs: 'Operation' and 'Administration'. Below the tabs are four buttons: 'Revoke Share', 'Generate New Key', 'Activate New Key', and 'Copy Files'. The 'Copy Files' button is selected, leading to the 'Copy Files' configuration page. This page has two main sections. The left section contains configuration fields: 'Modulus' (set to 'For192Bit'), 'NrOfShares' (16), 'Threshold' (3), 'Source Directory' (/home/thomas/Documents), 'Target Directory' (/home/thomas/tmp/backup), 'Status' (Key Generated), and a list of actions: '1) Combine Shares' (with a 'Combine' button), '2) Copy Files' (with a 'CopyFiles' button), and '3) Reset' (with a 'Reset' button). The 'Combine' and 'CopyFiles' buttons are circled in red. The right section shows a table with columns 'Index', 'Share', and 'Submit'. It contains three rows with 'Update' buttons. Below the table, there's a red-bordered box containing the following text: 'Current /home/thomas/workspace-sec/securefs/securefs-master/securefs-client-test/target/dir1/dir2/bigfile.iso.28', 'CopyFrom: /home/thomas/workspace-sec/securefs/securefs-master/securefs-client-test/target/dir1/dir2/bigfile.iso.28', 'Current /home/thomas/workspace-sec/securefs/securefs-master/securefs-client-test/target/dirCopy/dir2/bigfile.iso.28', and 'CopyTo: /home/thomas/workspace-sec/securefs/securefs-master/securefs-client-test/target/dirCopy/dir2/bigfile.iso.28'.

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.