



---

## Sicherheitsanforderungen an ein modernes, dezentrales Dateisynchronisationswerkzeug am Beispiel von »brig«

---

**Studenten:**

Christopher PAHL

Christoph PIECHULA

**Dozent:**

Prof. Dr. Thorsten SCHÖLER

# Inhaltsverzeichnis

<b>1</b>	<b>Abstract</b>	<b>1</b>
<b>2</b>	<b>Danksagung</b>	<b>2</b>
<b>3</b>	<b>Abbildungsverzeichnis</b>	<b>3</b>
<b>4</b>	<b>Abkürzungsverzeichnis</b>	<b>4</b>
<b>5</b>	<b>Einleitung</b>	<b>5</b>
5.1	Motivation . . . . .	5
5.2	Projektziel . . . . .	5
5.3	Zielgruppe . . . . .	5
5.4	Einsatzszenarien . . . . .	5
5.5	Der Name . . . . .	5
5.6	Lizenzierung . . . . .	5
<b>6</b>	<b>Stand der Technik</b>	<b>6</b>
6.1	Wissenschaftlicher Stand . . . . .	6
6.1.1	Sicherheit in P2P-Netzwerken . . . . .	6
6.1.2	Ähnliche Arbeiten: Bazil . . . . .	6
6.2	Konkurrenzanalyse . . . . .	6
6.2.1	Google Drive/encfs/cryfs . . . . .	6
6.2.2	Syncthing . . . . .	6
6.2.3	git-annex . . . . .	6
6.2.4	Btsync . . . . .	6
6.3	Problemstellung . . . . .	6
6.4	Gesellschaftliche und politische Aspekte . . . . .	6
6.5	Wahl der Sprache . . . . .	6
<b>7</b>	<b>Datensicherheit und Datenschutz</b>	<b>7</b>
<b>8</b>	<b>Sicherheitsaspekte an die Software</b>	<b>8</b>
8.1	Überblick über IPFS . . . . .	8
8.2	Metadatenübertragung über Seitenkanal . . . . .	8
8.2.1	XMPP . . . . .	8
8.2.2	MQTT . . . . .	8
8.3	Benutzerverwaltung . . . . .	8
<b>9</b>	<b>Anforderungen an die Sicherheit</b>	<b>9</b>
9.1	Authentifizierung . . . . .	9
9.1.1	Die brig ID . . . . .	9

9.1.2	Registrierung . . . . .	9
9.1.3	Zweifaktorauthentifizierung . . . . .	9
9.2	Validierung . . . . .	9
9.3	Authorisierung . . . . .	9
9.3.1	Partieller Zugriff auf Daten . . . . .	9
9.3.2	Master Keyfile für Unternehmen . . . . .	9
9.4	Datenverschlüsselung . . . . .	9
9.4.1	AES GCM, Chacha20/Poly1305 . . . . .	9
9.4.2	Streaming und wahlfreier Zugriff . . . . .	9
9.5	Datenintegrität . . . . .	9
9.6	Anforderung nach Anwender . . . . .	9
9.6.1	Heimanwender . . . . .	9
9.6.2	Unternehmen . . . . .	9
<b>10</b>	<b>Sicherheitsmodell von brig</b>	<b>10</b>
10.1	Sicherheitsannahmen . . . . .	10
10.1.1	Disclaimer . . . . .	10
10.2	Key Management . . . . .	10
10.2.1	Ableitung der Schlüssel . . . . .	10
10.2.2	Dezentrale Schlüsselverteilung . . . . .	10
10.3	Angriffszenarien . . . . .	10
10.4	Risikomanagement . . . . .	10
<b>11</b>	<b>Sicherheit und Usability</b>	<b>11</b>
11.1	FUSE Layer und Backend . . . . .	11
11.2	Grafische Oberflächen . . . . .	11
<b>12</b>	<b>Ausblick</b>	<b>12</b>
12.1	Kritische Betrachtung . . . . .	12
12.2	Weitere Entwicklung . . . . .	12
12.3	Wirtschaftliche Verwertung . . . . .	12
<b>13</b>	<b>Anhänge</b>	<b>13</b>









5.1 Motivation

5.2 Projektziel

5.3 Zielgruppe

5.4 Einsatzszenarien

5.5 Der Name

5.6 Lizenzierung



## 6 Stand der Technik

### 6.1 Wissenschaftlicher Stand

#### 6.1.1 Sicherheit in P2P-Netzwerken

#### 6.1.2 Ähnliche Arbeiten: Bazil

### 6.2 Konkurrenzanalyse

#### 6.2.1 Google Drive/encfs/cryfs

#### 6.2.2 Syncthing

#### 6.2.3 git-annex

#### 6.2.4 Btsync

### 6.3 Problemstellung

### 6.4 Gesellschaftliche und politische Aspekte

### 6.5 Wahl der Sprache



## **8    Sicherheitsaspekte an die Software**

### **8.1 Überblick über IPFS**

### **8.2 Metadatenübertragung über Seitenkanal**

#### **8.2.1 XMPP**

#### **8.2.2 MQTT**

### **8.3 Benutzerverwaltung**

## 9.1 Authentifizierung

### 9.1.1 Die brig ID

### 9.1.2 Registrierung

### 9.1.3 Zweifaktorauthentifizierung

## 9.2 Validierung

## 9.3 Authorisierung

### 9.3.1 Partieller Zugriff auf Daten

### 9.3.2 Master Keyfile für Unternehmen

## 9.4 Datenverschlüsselung

### 9.4.1 AES GCM, Chacha20/Poly1305

### 9.4.2 Streaming und wahlfreier Zugriff

## 9.5 Datenintegrität

## 9.6 Anforderung nach Anwender

### 9.6.1 Heimanwender

### 9.6.2 Unternehmen

**10.1 Sicherheitsannahmen****10.1.1 Disclaimer****10.2 Key Management****10.2.1 Ableitung der Schlüssel****10.2.2 Dezentrale Schlüsselverteilung****10.3 Angriffsszenarien****10.4 Risikomanagement**

## 11.1 FUSE Layer und Backend

## 11.2 Grafische Oberflächen

12.1 Kritische Betrachtung

12.2 Weitere Entwicklung

12.3 Wirtschaftliche Verwertung

