



Im Moment 0x01, kann bei inkompatiblen Änderungen inkrementiert werden.

Mögliche Werte:
0: ChaCha20
1: AES GCM

Mögliche Schlüssellängen sind abhängig von der verwendeten Cipher.

Nonce: öffentlicher Wert, der eindeutig sein muss. Entspricht bei brig dem Blockindex.

Länge des Paddings ist abhängig vom verwendeten Algorithmus.