Payload Format

- Version (1 byte)
  - Fixed: 0x03
- KDF parameters (17 byte)
  - KDF rounds log2 (1 byte)
  - Salt (16 byte)
- Ciphertext (38 byte plain, 38/48 byte encrypted)
  - PurposeId (4 byte)
  - Entropy (32 byte)
  - Checksum (2 byte)
    - blake2b(purposeId + entropy)[0..2]
- Total: 56 byte plain, 56/66 byte encrypted

Algorithms Option 1

- KDF
  - pbkdf2
  - Output size: 48 byte (256bit + 128bit IV)
- Encryption
  - aes-256-cbc

- Pros
  - Easiest to implement
- Cons
  - Pbkdf2 is old and there are known acceleration attacks
  - AES pads output to block size, increasing ciphertext size

Algorithms Option 2

- KDF
  - argon2d
  - Output size: 38 byte
- Encryption
  - One time pad (xor)

- Pros
  - State of the art KDF
  - Smaller ciphertext size
- Cons
  - More effort required to implement Argon2d efficiently