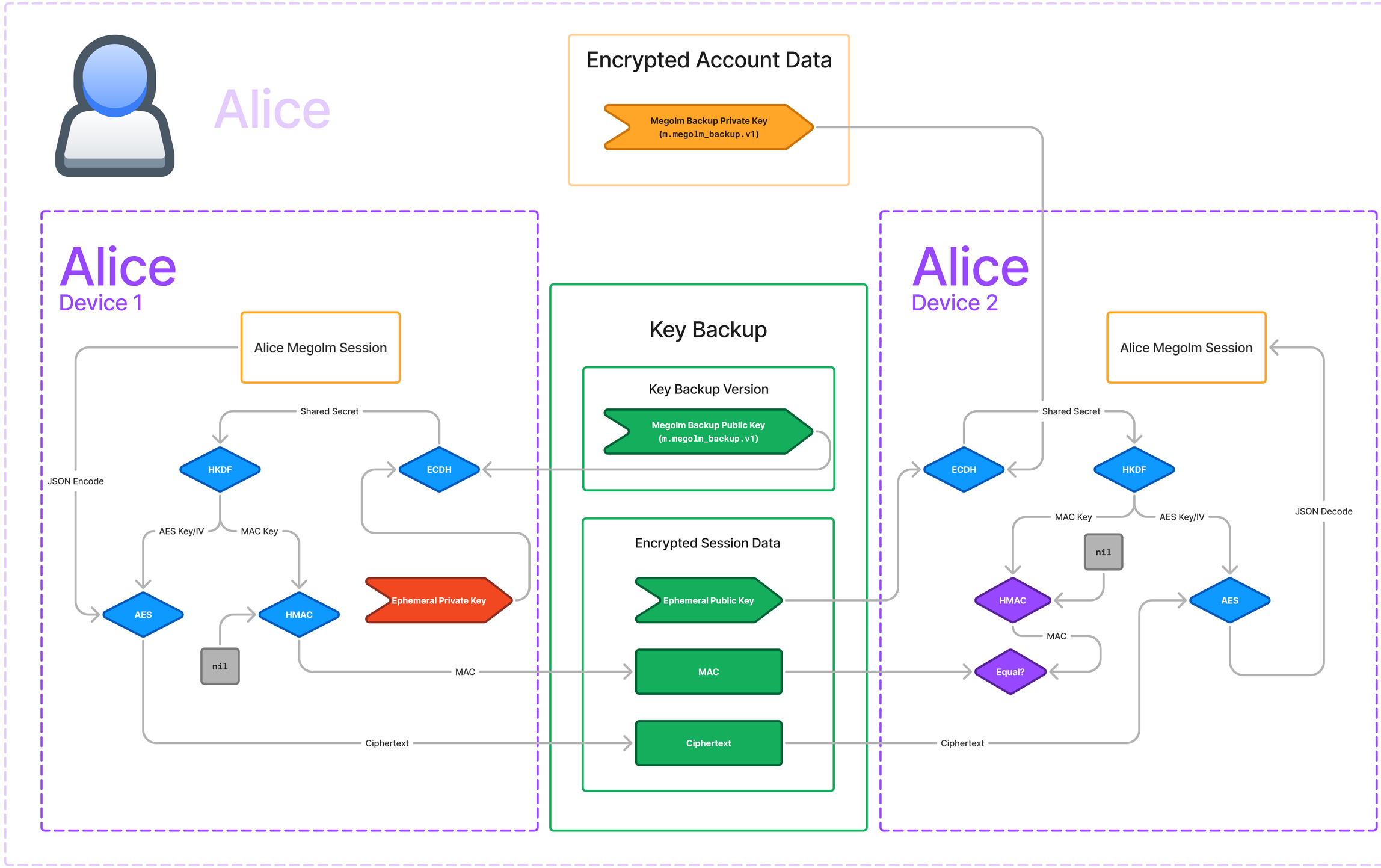
Alice
Encrypted Account Data
Megolm Backup Private Key
(m.megolm_backup.v1)
Alice
Device 1
Alice Megolm Session
Shared Secret
HKDF
ECDH
JSON Encode
AES Key/IV
MAC Key
AES
HMAC
Ephemeral Private Key
nil
MAC
Ciphertext
Key Backup
Key Backup Version
Megolm Backup Public Key
(m.megolm_backup.v1)
Encrypted Session Data
Ephemeral Public Key
MAC
Ciphertext
Alice
Device 2
Alice Megolm Session
Shared Secret
ECDH
HKDF
MAC Key
AES Key/IV
nil
HMAC
AES
MAC
Equal?
JSON Decode
Ciphertext