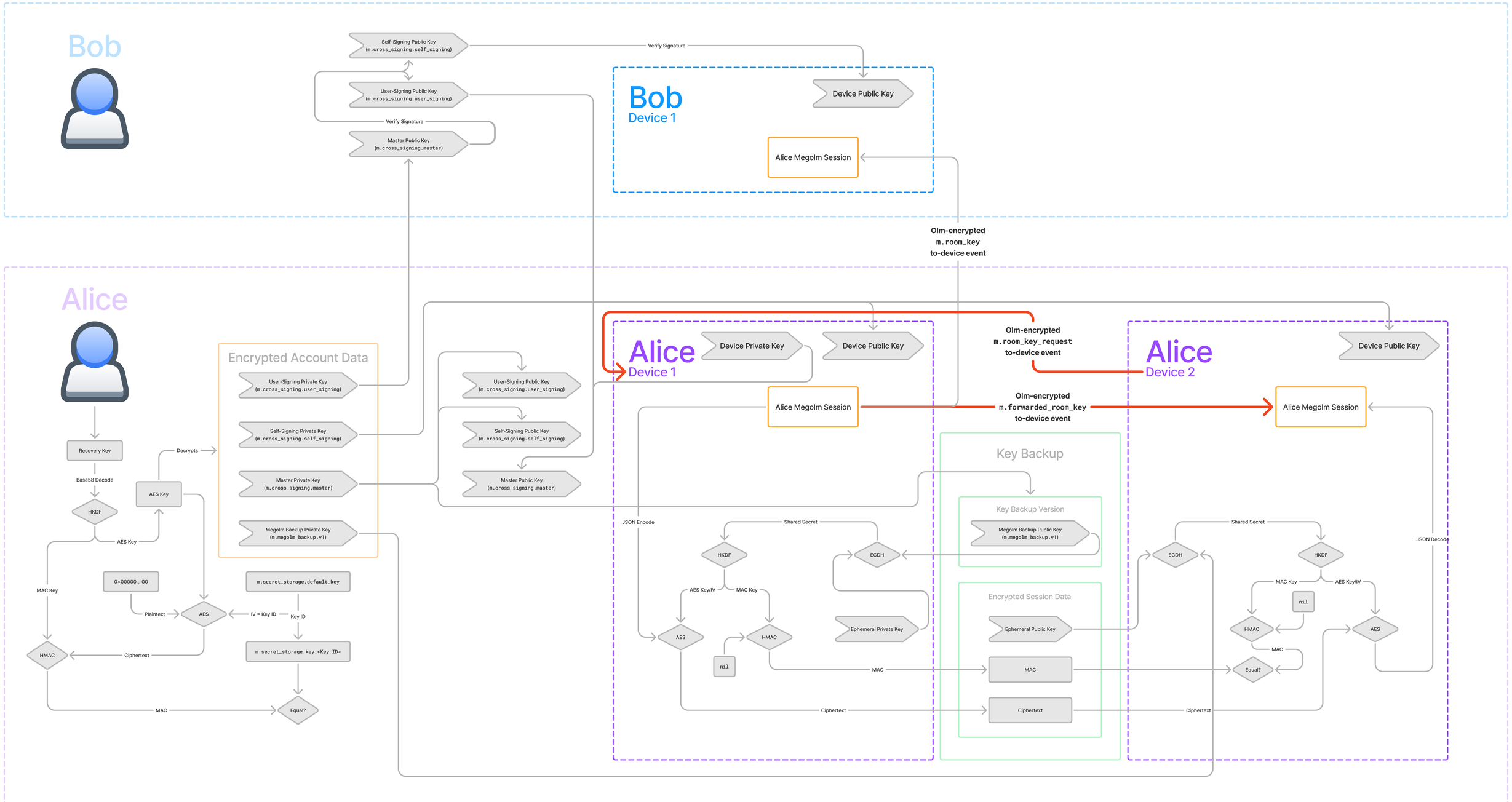
Bob
Self-Signing Public Key
(m.cross_signing.self_signing)
Verify Signature
User-Signing Public Key
(m.cross_signing.user_signing)
Verify Signature
Master Public Key
(m.cross_signing.master)
Bob
Device 1
Device Public Key
Alice Megolm Session
Olm-encrypted
m.room_key
to-device event
Alice
Encrypted Account Data
User-Signing Private Key
(m.cross_signing.user_signing)
Self-Signing Private Key
(m.cross_signing.self_signing)
Master Private Key
(m.cross_signing.master)
Megolm Backup Private Key
(m.megolm_backup.v1)
User-Signing Public Key
(m.cross_signing.user_signing)
Self-Signing Public Key
(m.cross_signing.self_signing)
Master Public Key
(m.cross_signing.master)
Recovery Key
BaseS8 Decode
HKDF
AES Key
Decrypts
AES Key
MAC Key
0x00000....00
Plaintext
AES
IV = Key ID
Key ID
m.secret_storage.default_key
m.secret_storage.key.<Key ID>
HMAC
Ciphertext
MAC
Equal?
Alice
Device 1
Device Private Key
Device Public Key
Alice Megolm Session
JSON Encode
Shared Secret
HKDF
ECDH
AES Key/IV
MAC Key
AES
HMAC
nil
Ephemeral Private Key
MAC
Ciphertext
Olm-encrypted
m.room_key_request
to-device event
Olm-encrypted
m.forwarded_room_key
to-device event
Key Backup
Key Backup Version
Megolm Backup Public Key
(m.megolm_backup.v1)
Encrypted Session Data
Ephemeral Public Key
MAC
Ciphertext
Alice
Device 2
Device Public Key
Alice Megolm Session
Shared Secret
ECDH
HKDF
JSON Decode
MAC Key
AES Key/IV
nil
HMAC
AES
MAC
Equal?
Ciphertext