Digital Lisa Club – ANCHOR’ s

ENC-Wallet.json – Explanation & Usage

1. What is the ENC-Wallet.json file?

The ENC-Wallet.json file is not a true wallet, but rather a utility file required within the Anchor system to securely manage encrypted HQ files (HQ-ENC).ÿÿIt serves as an interface between the owner's Bitcoin signature (BIP-322) and the encrypted files (ENCs) belonging to an Anchor.

In short:

The ENC-Wallet.json is a technical identity file that allows the system to know which public key may be used to decrypt an encrypted asset.

2. When and why do you need an ENC wallet?

An ENC-Wallet.json file is always required when:

- an anchor that mints or buys an anchor that uses or contains an HQ-ENC file,
- or if you want to sell such an anchor.

ENC-Wallet.json allows the system to perform secure key wraps without having to read your hardware wallet.

3. Why is it necessary?

When an anchor file containing an encrypted HQ file is sold, a new encryption key (keywrap) must be generated upon change of ownership. This keywrap is based on a signature of the buyer (canonical message), which can later decrypt the Content Encryption Key (CEK).

To ensure this works reliably:

- This signature of the buyer must never be made public.
- Therefore, it is encrypted and written to the seller's public key (from their ENC-Wallet.json).

Only the seller can decrypt this encrypted signature using the Dapp.

This ensures that only the current owner has access to the sensitive data.

4. Why not a hardware wallet?

The ENC-Wallet.json file must not be based on a hardware wallet (Ledger, Trezor, etc.) because:

- You must have access to the private key of the generated public key.
- and hardware wallets never release this information.

Therefore, the ENC wallet key is always created with the AnchorKey Generator – either offline or online.

5. Creating an ENC-Wallet.json (step-by-step))

Part 1 —Generating Offline Keypair

1. Open AnchorKey OFFLINE.html (runs completely without an internet connection).
2. Click on Generate Keypair.

--> A fully functional Bitcoin BIP-322 key pair is generated:

- Address
- Public Key
- Private Key

3. Then click on Download Encrypted Keypair.

- Choose or generate a secure password.
- Click on Encrypt & Download.

Your browser is now downloading 3 files:

PubKey+Address-for-Import_YYYY-MM-DD.txt

Password_For_Encrypted_Key_YYYY-MM-DD.txt

Encrypted_Private_Key_YYYY-MM-DD.txt

4. Backup of files:

- Keep Password_For_Encrypted_Key... and Encrypted_Private_Key... on two different USB sticks.
- The USB sticks must be stored separately.
- No one can do anything with the encrypted private key as long as the password is unknown.

Part 2 —Creating ENC-Wallet.json

1. Open AnchorKey ONLINE.
2. Click on Import Data and select the file
   PubKey+Address-for-Import_YYYY-MM-DD.txt.
3. Enter your own Bitcoin address under “ Enter your BTC address” .
4. Click on Generate ENC-Wallet.json.

   --> The system generates a signature message.
5. Sign this message in your Bitcoin wallet (e.g. Sparrow) using BIP-322.
6. Paste the generated signature into the field “ Enter BIP322 signature…” .
7. Click on Verify Signature.

   If the signature is valid, the button will appear:

   Upload ENC-Wallet-TX

   --> This button uploads the ENC wallet file (.json) to Arweave.

6. What happens if you lose data?

- If you lose your ENC wallet files or password,

  You can create a new ENC-Wallet.json at any time.

- The new version will be used automatically as soon as you receive a new offer or an anchor mint.
- Important : If you have already received a purchase offer with an encrypted signature, but this signature was created with your old ENC wallet, then it can no longer be decrypted with a new one.

In this case, the buyer must recreate the offer so that your new ENC wallet can be used.

7. Validity and Reuse

A single ENC-Wallet.json file is sufficient, regardless of how many collections or anchors you own or mint.
It only serves to tell the system:

"This user possesses a verified key that can be used for secure encryption and decryption."

8. Safety and Recommendation

- Always use a hardware wallet (Ledger, Trezor, etc.) for your real Anchors.
- Use the ENC-Wallet.json solely as a technical bridge between your ownership address and the encrypted files.
- Store passwords and encrypted keys separately.
- Signatures should never be stored long-term, but recreated as needed.

9. Summary

Step	Description
What	Technical JSON file for managing encrypted HQ files
When necessary	When minting, buying or selling anchors with HQ-ENC
Why	So that keys can be securely transferred between owners
Created with	AnchorKey OFFLINE (Keypair) + AnchorKey ONLINE (ENC wallet.json)
Linking to wallet	Not a real wallet! Just a similar name.
Security	PrivKey is encrypted, signature verification via BIP-322, no hardware wallet required.
Reuse	One ENC-Wallet.json file is sufficient for all anchors belonging to the same owner.