AnchorVerse

KeyWrap & Ticket JSON —Explanation & Usage

1. What is a KeyWrap?

A KeyWrap is a core security component that enables access to encrypted HQ files (HQ-ENC) linked to an Anchor.

It contains the encrypted Content Encryption Key (CEK), which can only be unlocked using a valid Bitcoin signature (BIP-322) from the current owner.

This ensures:

- No private keys will be disclosed.
- Access is granted exclusively via signatures.

2. What is a Ticket JSON?

A Ticket JSON is created by the new owner and is required to generate a new KeyWrap.

It includes:

- a canonical message signature
- encrypted with the public key of the seller or creator

Depending on the situation, it is created via:

- automatic generation (offers)
- or manually via
  Change Ownership Address.html DApp
  Card:
  Create & Upload Ticket for KeyWrap after Intent - Self Transfer / Airdrop

Optional offline processing via:
Create Ticket OFFLINE.html DApp

3. Relationship between Anchor, KeyWrap, and Ticket

To access an encrypted file:

- a valid KeyWrap is required
- plus a valid Bitcoin signatureplus a valid Bitcoin signature

A new KeyWrap is required after every ownership change.
The Ticket provides the required input.

In short:

- Ticket -> provides the encrypted authorization
- KeyWrap -> enables actual access

4. Decryption of HQ-ENC Files

The decryption process is fully automated inside the DApp:

TheDApp:

- checks the owner status
- loads the ENC file and KeyWrap from Arweave
- displays the canonical message for the signature.

After signing:

- the CEK is decrypted from the KeyWrap
- the file is decrypted locally
- and made available for download

This process runs within the viewer/decrypt function of the DApp,

without manual key management.

5. KeyWrap Creation (Sale / Lending)

During a sale or lending process:

- a Ticket is automatically created
- the seller processes it using:

Seller.html DApp and **AnchorKey OFFLINE.html DApp**

Inside the offline DApp, the Card:

Create KeyWrap JSON

is used to generate the new KeyWrap.

Upload is done via **Seller.html DApp.**

6. Self-Transfer / Airdrop

In the case of a direct transfer (without an offer), no automatic ticket is generated.
The new owner must create one themselves via:

Change Ownership Address.html DApp

Card:

Create & Upload Ticket for KeyWrap after Intent - Self Transfer / Airdrop

Optionally, the ticket can also be processed offline via:

Create Ticket OFFLINE.html DApp

The previous owner then uses this ticket, as with a normal sale, to create a new KeyWrap.

7. Fallback: If no keywrap is created

If no KeyWrap is created:

The owner can generate new Tickets via:

AnchorKey ONLINE.html DApp

Card:

Find PubKey to Create New Ticket

The appropriate public key will be loaded automatically.

The actual ticket creation then takes place in:

AnchorKey OFFLINE.html DApp

Card:

Create Ticket.json for Creator / Seller

The completed tickets will be uploaded again via:

AnchorKey ONLINE.html DApp

Card:

Upload New Ticket.json

These tickets can be used either:

- by the seller

- or by the creator

8. Security and Recommendation

The creator performs a backup function within the system.

They can process tickets and create new KeyWraps if sellers become unavailable.
For this, they use the:

New Ticket JSON.html DApp

This DApp enables:

- automatic checking for the existence of new tickets

- verification of whether the ticket creator is the owner

Processing then takes place in the:

AnchorKey OFFLINE.html DApp

Card:

Create KeyWrap JSON MASS Upload for Creators

The completed KeyWraps are uploaded via:

AnchorKey ONLINE.html DApp

Card:

KeyWrap MASS Upload for Creators

9. Security and System Logic

The system is based on the following principles:ÿ

- Tickets are always encrypted for exactly one public key
- Only the matching private key can decrypt them
- KeyWraps never contain unencrypted keys
- Access is via signatures, not wallet access

Additionally:

- Critical processes run through the **AnchorKey OFFLINE.html DApp**
- This can be operated completely offline or on air-gapped systems

10. Summary

KeyWrap and ticket together form the basis for:

- Secure delivery of encrypted content
- Access control through signatures
- Independent recovery by the creator

The DApps are clearly divided:

- Downloads & upload -> ONLINE DApps
- Cryptographic processing -> OFFLINE DApps
- Sales / transfer -> Seller DApp

11. Further Information

Detailed information on all DApps:
https://app.anchorverse.io