AnchorVerse

KeyWrap & Ticket JSON —Erklärung & Nutzung

1. Was ist ein KeyWrap?

Ein KeyWrap ist eine zentrale Sicherheitskomponente im AnchorVerse-Ökosystem.
Er ermöglicht den Zugriff auf verschlüsselte HQ-Dateien (HQ-ENC), die einem Anchor zugeordnet sind.

Technisch enthält der KeyWrap den **verschlüsselten Content Encryption Key (CEK)**.
Dieser kann ausschließlich durch eine gültige **Bitcoin-Signatur (BIP-322)** des aktuellen Besitzers entschlüsselt werden.
Dadurch wird sichergestellt:

- Keine privaten Schlüssel werden offengelegt
- Zugriff erfolgt ausschließlich über Signaturen

2. Was ist ein Ticket JSON?

Ein Ticket JSON ist eine vorbereitende Datei für die Erstellung eines neuen KeyWraps bei einem Besitzerwechsel.

Es wird vom neuen Besitzer erzeugt und enthält:

- eine Canonical Message Signatur
- verschlüsselt mit dem Public Key des Empfängers (Seller oder Creator)

Die Erstellung erfolgt je nach Situation über unterschiedliche DApps:

- Bei normalen Verkäufen automatisch im Hintergrund
- Bei manuellen Transfers über die
  Change Ownership Address.html DApp
  in der Card:
  Create & Upload Ticket for KeyWrap after Intent - Self Transfer / Airdrop

Optional kann das Ticket zusätzlich über die
Create Ticket OFFLINE.html DApp
offline vervollständigt werden.

3. Zusammenhang zwischen Anchor, KeyWrap und Ticket

Ein Anchor mit HQ-ENC benötigt zur Nutzung:

- eine gültige KeyWrap
- eine gültige Bitcoin-Signatur des Besitzers

Der KeyWrap wird bei jedem Besitzerwechsel neu erstellt.
Das Ticket ist dabei die notwendige Grundlage für diese Erstellung.

Kurz:

- Ticket -> liefert die verschlüsselte Berechtigung
- KeyWrap -> ermöglicht den tatsächlichen Zugriff

4. Entschlüsselung eines HQ-ENC Files

Die Entschlüsselung erfolgt direkt in der DApp und ist vollständig automatisiert.

Die DApp:

- prüft den Besitzerstatus
- lädt ENC-Datei und KeyWrap von Arweave
- zeigt die Canonical Message zur Signatur an

Nach der Signatur:

- wird der CEK aus dem KeyWrap entschlüsselt
- die Datei lokal entschlüsselt
- und zum Download bereitgestellt

Dieser Prozess läuft innerhalb der Viewer-/Decrypt-Funktion der DApp, ohne manuelle Schlüsselverwaltung.

5. Erstellung eines KeyWraps bei Verkauf oder Verleih

Bei einem Verkauf oder Lending-Prozess (DApp Offer / Lend):

- wird das Ticket automatisch erzeugt, sobald ein Käufer ein Angebot erstellt
- dieses Ticket gehört bereits dem neuen Besitzer

Der Verkäufer arbeitet anschließend mit:

- der **Seller.html DApp**
- sowie der **AnchorKey OFFLINE.html DApp**

In der Offline-DApp wird in der Card:

Create KeyWrap JSONdas Ticket zusammen mit der bestehenden KeyWrap importiert.

Dort wird die neue KeyWrap für den neuen Besitzer erzeugt.

Der Upload erfolgt anschließend wieder über die **Seller.html DApp**,

welche die neue KeyWrap auf Arweave speichert.

6. Self-Transfer und Airdrop

Bei einem direkten Transfer (ohne Offer) existiert kein automatisches Ticket.

Der neue Besitzer muss dieses selbst erstellen über die:

Change Ownership Address.html DApp

Card:

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

Optional kann das Ticket zusätzlich über die:

Create Ticket OFFLINE.html DApp

offline verarbeitet werden.

Der vorherige Besitzer nutzt dieses Ticket anschließend wie bei einem normalen Verkauf,

um eine neue KeyWrap zu erstellen.

7. Fallback: Wenn keine KeyWrap erstellt wird

Falls kein Verkäufer reagiert oder keine KeyWrap existiert, bleibt der neue Besitzer handlungsfähig.

Er kann neue Tickets erzeugen über die:

AnchorKey ONLINE.html DApp

Card:

Find PubKey to Create New Ticket

Dort wird automatisch der passende Public Key geladen.

Die eigentliche Ticket-Erstellung erfolgt anschließend in der:

AnchorKey OFFLINE.html DApp

Card:

Create Ticket.json for Creator / Seller

Die fertigen Tickets werden wieder hochgeladen über:

AnchorKey ONLINE.html DApp

Card:

Upload New Ticket.json

Diese Tickets können entweder:

- vom Verkäufer
- oder vom Creator genutzt werden

8. Sicherheit und Empfehlung

Der Creator übernimmt eine Backup-Funktion im System.

Er kann Tickets verarbeiten und neue KeyWraps erstellen, falls Verkäufer ausfallen.

Dafür nutzt er die:

New Ticket JSON.html DApp

Diese DApp ermöglicht es:

- automatisch zu prüfen, ob neue Tickets existieren
- zu verifizieren, ob der Ticket-Ersteller der Owner ist

Die Verarbeitung erfolgt anschließend in der:

AnchorKey OFFLINE.html DApp

Card:

Create KeyWrap JSON MASS Upload for Creators

Die fertigen KeyWraps werden hochgeladen über:

AnchorKey ONLINE.html DApp

Card:

KeyWrap MASS Upload for Creators

9. Sicherheit und Systemlogik

Das System basiert auf folgenden Prinzipien:

- Tickets sind immer für genau einen Public Key verschlüsselt
- Nur der passende Private Key kann sie entschlüsseln
- KeyWraps enthalten niemals unverschlüsselte Schlüssel
- Zugriff erfolgt über Signaturen, nicht über Wallet-Zugriff

Zusätzlich:

- Kritische Prozesse laufen über die **AnchorKey OFFLINE.html DApp**
- Diese kann vollständig offline oder auf Air-Gapped Systemen betrieben werden

10. Zusammenfassung

KeyWrap und Ticket bilden gemeinsam die Grundlage für:

- sichere Übergabe von verschlüsselten Inhalten
- Zugriffskontrolle durch Signatur
- unabhängige Wiederherstellung durch Creator

Die DApps sind dabei klar aufgeteilt:

- Downloads & Upload -> ONLINE DApps
- Kryptografische Verarbeitung -> OFFLINE DApps
- Verkauf / Übergabe Seller DApp

11. Weitere Informationen

Detailierte Informationen zu allen DApps:

https://app.anchorverse.io