

全線上 AI 肖像素材授權撮合平台

功能框架・安全體系・實施路徑

平台不做買賣、只做撮合與基礎設施：創作者端一鍵上傳肖像並完成確權，使用方按需購買授權並取得「一授權一密鑰」，全鏈路可追溯、可核驗、可維權。

文件版本 v1.0 更新日期 2026-09-15 適用對象 客戶 / 合作機構 / 投資人

形態 H5 + Android APP + 管理後台

01 產品定位與三方角色

平台是「肖像權的合規交易所」：把線下影棚採集、人工談授權、紙質合同的全過程，搬到線上由技術完成確權、加密、授權與結算。

創作者（C 端）

CREATOR

肖像權持有人，提供合規素材並取得收益。

- ▶ 實名認證 + 活體核驗，杜絕盜臉
- ▶ 手機引導拍攝，無需影棚與專業燈光
- ▶ 作品審核後加密入庫、鏈上確權
- ▶ 自主定價、按授權次數持續分成 85%

使用方（B 端）

LICENSEE

AI 短劇、數字人、廣告等需要合規人像的機構。

- ▶ 按場景篩選素材，明碼標價、在線授權
- ▶ 取得專屬密鑰，憑密鑰調取高精度素材
- ▶ API 對接，素材直接流入自有生產線
- ▶ 授權書與存證編號可審計，降低法律風險

平台（撮合方）

PLATFORM

不做買賣、不持有肖像權，提供撮合與安全基礎設施。

- ▶ 審核質檢、加密保險庫、密鑰簽發
- ▶ 資金托管（ESCROW）與合規分賬 15%
- ▶ 全鏈路追溯審計、爭議取證支持
- ▶ 開放 API 與 ERP/CRM 運營中台

02 端到端業務閉環（八步路徑）

從一次上傳到一筆結算，每一步都有對應的技術動作與安全措施，形成可審計的完整鏈路。



03 功能框架路徑圖（三層架構）

用戶端負責體驗與交易，平台能力層負責安全與自動化，管理端負責運營與風控。三層之間以 API 與事件流打通。



數據看板

GMV · 活躍 · 趨勢

授權訂單

狀態流轉 · 退款爭議

素材審核

待審隊列 · 駁回理由

創作者 CRM

分層運營 · 激勵

機構 CRM

續約 · 用量 · 服務

分賬結算

85/15 · T+1 · 對帳

支付通道

微信 · 支付寶配置

密鑰追溯

密鑰台賬 · 鏈上存證

04 安全體系：十道防線

對客戶最常被問到的問題——「用 AI 生成的臉，怎樣證明是我授權？怎樣防止被人盜用？被盜了怎麼辦？」——平台用十層技術逐層回答。

D-01 源頭真實性

註冊實名認證 + 活體動作核驗，確保上傳者就是肖像權本人；動態核驗令照片、面具、Deepfake 無法通過。

對應模組：活體核驗 · 實名認證 · 權利人 DID

D-02 存儲加密

審核通過即刻以 AES-256 加密入庫，平台側不落明文原文；密文與密鑰分離保存，內部人員亦無法直接取得原圖。

對應模組：加密保險庫 · 密文分片存儲

D-03 訪問控制（生物特徵鎖）

創作者本人以設備指紋 / Face ID / Windows Hello 驗證身份，通過後才解鎖自己的作品資料庫；生物特徵在本機驗證器完成比對，**不出設備、平台不存生物數據**。

對應模組：生物特徵鎖（WebAuthn 平台驗證器）

D-04 密鑰治理：一授權一密鑰

每一筆授權簽發一條專屬密鑰，唯一綁定「該作品 + 該授權範圍 + 該使用方」。再做另一筆授權就是另一條全新密鑰，絕不重用；平台側僅保存哈希，密鑰原文不可逆。

對應模組：密鑰簽發（SHA-256）· 撤銷即時失效（403）

D-05 全鏈路追溯

每次用密鑰調取素材都寫入追溯日誌：時間、密鑰、作品、使用方、行為、結果。素材疊加隱形水印，一旦外洩可反查到具體是哪條密鑰流出。

對應模組：追溯日誌 · 隱形水印 · 異常調用告警

D-06 區塊鏈確權

作品原文不上鏈，只把「內容指紋 + 權利人 DID + 授權條款哈希」錨定聯盟鏈，多筆聚合 Merkle 根降低成本；確權、授權、撤銷三類事件全部上鏈留痕，出具可對外核驗的數碼確權證書。

對應模組：鏈上確權 · 確權證書 · 司法鏈核驗（無代幣）

D-07 糾紛解決與舉證支持

發生侵權爭議時，平台可一次性輸出完整證據包：確權存證編號與交易哈希、授權合同與條款哈希、密鑰簽發與調用日誌、水印反查結論。四項互相印證，形成可提交法院的電子證據鏈，而不是只有一張截圖。

對應模組：取證報告導出 · 存證編號在線核驗 · 電子證據鏈（密鑰 + 日誌 + 水印 + 鏈上存證）

D-08 脫敏特徵與防改臉盜用

原始人臉素材 AES-256 加密隔離、永不外流；對外只輸出注入水印的脫敏特徵向量（106 關鍵點 → 512 維）——生成方拿不到原圖，也無法從向量還原人臉。就算有人微調「改臉」盜用，骨骼關鍵點與五官拓撲比對 + 向量水印反解依然命中，鎖定洩露授權並出具相似度報告：改得掉五官，改不掉骨骼拓撲與水印。權利人還可自訂題材黑名單（哈希寫入授權條款），一鍵銷毀向量即刻斷供並取得銷毀證書；一項目一授權，到期向量副本強制銷毀。

銷毀採兩段式閉環：僅權利人生物驗證可發起 → 即時凍結斷供（403）→ 7 日申訴期內使用方以授權密鑰、合同、鏈上存證編號自證（簽約即自動持有，零成本舉證）→ 期滿才物理銷毀並出具銷毀證書；申訴成立則從隔離區原始素材重新提取恢復並追責誤毀。平台只留痕、不做裁判，爭議升級版權仲裁機構與司法鏈。

對應模組：脫敏提取流水線 · 向量水印 · 反向溯源比對 · 題材黑名單 · 一鍵銷毀與銷毀證書 · 到期強制銷毀

D-09 全網侵權監測雷達

向量水印反解 + 骨骼拓撲比對 + 感知哈希三重特徵索引，7×24 掃描社交、視頻、電商與 AI 生成平台，主動發現盜用——普通圖搜抓不到的 AI 改臉同樣命中，發現即自動出具相似度報告並告警權利人。

對應模組：監測任務配置 · 命中告警推送 · 相似度報告自動生成

D-10 一鍵維權下架

命中證據自動打包為投訴函與律師函範本，向侵權平台批量發起投訴下架，進度全程可追蹤並上鏈歸檔；必要時移交版權仲裁與司法通道，維權收益可與權利人按約分成。

對應模組：證據包一鍵組裝 · 批量投訴下架 · 維權進度追蹤

D-06 架構圖：區塊鏈數據確權路徑



原文不上鏈 · 只錨定指紋 · 確權 / 授權 / 撤銷事件全留痕

05 資金安全與分賬機制

交易資金全程托管，平台只在授權生效後按比例抽取服務佣金，不經手自有資金池。

資金托管 ESCROW 使用方支付後資金進入平台托管帳戶，授權交付完成才解付；如授權失敗或爭議成立，原路退回。	分賬比例 REVENUE SPLIT 創作者 85% · 平台服務佣金 15%，按每筆授權獨立計算，明細可查、可對帳。
結算通道 SETTLEMENT 對接微信支付 / 支付寶持牌通道，分賬與 T+1 結算；平台側保留完整對帳單與提現流水。	

06 合規底線（可對客戶明確承諾）

以下為平台對外可作出的明確合規承諾，也是與客戶簽約時可直接引用的條款要點。

項目	平台做法	客戶可獲得
肖像權本人同意	實名 + 活體核驗 + 授權範圍明確勾選並留存記錄	授權書 + 存證編號
個人信息保護	原文加密、生物特徵不出設備、最小必要原則授權	合規採購憑證
脫敏特徵 · 防盜用	原始素材隔離、對外只出脫敏向量；題材黑名單寫入條款、向量可銷毀並出具銷毀證書	改臉也逃不掉 · 盜用必留痕
數據知識產權登記	支持為作品與授權辦理數據知識產權登記，登記編號與鏈上存證互相印證	登記憑證可出示
授權可撤銷	創作者可撤銷授權，密鑰即時失效，使用方調用返回 403	明確的權利邊界
區塊鏈服務合規	採用無代幣聯盟鏈存證，不涉及任何代幣發行與交易	可核驗的電子證據
數據不出境 / 可審計	境內存儲與節點部署，全程操作日誌留存、可導出對帳與取證報告	審計友好
使用範圍限制	按授權類型（商用 / 數字傳播 / 全權益）限定用途、期限與地域	越界即違約可追責

07 實施路線圖

分期推進：先跑通撮合與確權閉環，再規模化素材供給與機構對接，最後做生態與版權流轉。

○ 第一階段・閉環驗證 (MVP) PHASE 1 · 0-6 個月

上線 H5 + Android APP：實名註冊、引導採集、審核入庫、素材市場、在線授權、密鑰簽發、追溯日誌、85/15 分賬；完成加密保險庫與生物特徵鎖；ERP/CRM 管理後台投入使用。目標：驗證 C 端素材供給與 B 端付費意願。

○ 第二階段・規模化與機構對接 PHASE 2 · 6-18 個月

上線 API 開放平台，對接 AI 短劇、數字人、廣告等機構；區塊鏈確權對接司法鏈並完成存證核驗；開通微信 / 支付寶持牌分賬；建立創作者分層運營與激勵體系；擴充多風格、多角度標準化素材庫。

○ 第三階段・生態與版權流轉 PHASE 3 · 18-36 個月

探索肖像權二次授權與跨平台流轉、與版權交易機構 / 公證機構 / 保險機構合作；沉澱行業標準化的肖像授權與存證規範；以數據服務與風控能力形成平台護城河。

08 技術底座與形態

全線上、零線下影棚；同一套前端代碼同時輸出網頁、H5 與原生安裝包。

形態

DELIVERY

單頁應用（主站）+ 輕量 H5 + Android APK 安裝包，三端功能一致。

運行方式

RUNTIME

瀏覽器直接運行，零外部依賴；安裝包離線可用，適合演示與駐場。

中台

ERP / CRM

九大模組覆蓋運營全流程：看板、訂單、審核、CRM、分賬、支付、API、密鑰追溯。

開放能力

OPEN API

REST + HMAC 簽名 + Webhook 事件，機構素材可直接流入自有生產線。

一句話總結

平台的核心不是「賣圖」，而是「賣一份可證明、可追溯、可舉證的授權」——創作者放心交付肖像，使用方放心拿去生產，出了爭議有完整證據鏈。