



# SANDJAR GROUP

## ATLAS PLATFORM

### DOCUMENT No. 8

## User Policy: Authorization & Verification Face ID — Formation of a Court-Admissible Structure

*Biometric Authentication, Payment Authorization, Legal Representation & Contractor Selection Framework*

|                      |                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------|
| Issued by:           | Atlas Overseas FZE                                                                      |
| Document Version:    | v1.0 — May 2026                                                                         |
| Legal Standard:      | UAE Federal Law No. 1 of 2006 (Electronic Commerce & Transactions); UAE Law of Evidence |
| Biometric Framework: | Face ID   ISO/IEC 30107-3 Liveness Detection   NIST SP 800-63B                          |
| Classification:      | Confidential & Proprietary — Legal & Technical Document                                 |

# I. PURPOSE & LEGAL FOUNDATION

This User Policy establishes the complete framework for user authorization, identity verification, biometric authentication, and digital signature on the ATLAS Platform. It is specifically designed to ensure that all Platform actions — including payments, contract execution, legal representation, and contractor selection — meet the evidentiary standards required by UAE courts and international legal proceedings.

## 1.1 Governing Legal Standards

| Legal Standard                                         | Application to ATLAS Authorization                                                                                                                               |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UAE Federal Law No. 1 of 2006 (E-Commerce)             | Establishes legal equivalence of electronic signatures and records with handwritten signatures and paper documents — basis for ATLAS e-signature enforceability. |
| UAE Federal Decree-Law No. 46 of 2021 (E-Transactions) | Updated electronic transactions law confirming admissibility of digital records and biometric-authenticated transactions as legal evidence.                      |
| UAE Federal Law No. 10 of 1992 (Law of Evidence)       | Governs admissibility of electronic evidence in UAE courts — ATLAS records are structured to meet Articles 17-20 authentication requirements.                    |
| NIST SP 800-63B (Digital Identity Guidelines)          | International standard for authentication assurance levels (AAL1–AAL3). ATLAS payment authorization targets AAL2 minimum for all financial transactions.         |
| ISO/IEC 30107-3 (Liveness Detection)                   | Standard for presentation attack detection in biometric systems. ATLAS Face ID system is certified to ISO/IEC 30107-3 Level 2.                                   |
| GDPR Article 9 / UAE PDPL                              | Biometric data is a special category — processing requires explicit consent and enhanced protection measures (see Document 5).                                   |
| FATF Guidance on Digital Identity                      | FATF's risk-based approach to digital identity for AML/KYC — ATLAS biometric KYC aligns with FATF Guidance on Digital Identity (2020).                           |

# II. FACE ID ARCHITECTURE — TECHNICAL & LEGAL FRAMEWORK

## 2.1 Three-Layer Authentication Stack

Every authorization action on the ATLAS Platform passes through a three-layer authentication stack. The combination of all three layers creates a court-admissible evidence chain that uniquely links the action to a verified individual.

| Layer | Component         | Technical Specification                                                                                                                                    | Evidence Value                                |
|-------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| 1     | Something You Are | Face ID biometric scan. ISO/IEC 30107-3 L2 liveness detection. 3D depth map + infrared (Apple TrueDepth equivalent). 1-in-1,000,000 false acceptance rate. | Links action to physical person biometrically |

|   |                           |                                                                                                                                                            |                                                     |
|---|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| 2 | <b>Something You Have</b> | Registered device (device ID + certificate pinning). ATLAS-issued session token (JWT, 15-min expiry). Push notification confirmation to registered mobile. | Confirms action from known, registered device       |
| 3 | <b>Something You Know</b> | 6-digit platform PIN (optional secondary factor for high-value transactions > AED 500,000). PIN never stored — salted hash only.                           | Adds knowledge-based barrier for large transactions |

## 2.2 Face ID Data — Collection, Storage & Protection

- Face ID mathematical template (not the raw image) is generated on-device using the platform SDK. The raw biometric image is never transmitted to ATLAS servers.
- The encrypted mathematical template is stored in the user's device secure enclave — accessible only to the ATLAS application with user consent.
- ATLAS servers receive only: a binary authentication result (pass/fail) + a session confirmation token. No biometric template or image is stored on ATLAS infrastructure.
- Template deletion: Face ID template is deleted from device secure enclave upon account closure, device change, or user request — within 90 days maximum.
- Biometric data is processed exclusively in the UAE. No cross-border transfer of biometric templates under any circumstances.
- Explicit consent for biometric processing is collected at onboarding — separate from general Terms acceptance, per GDPR Article 9 and UAE PDPL requirements.

# III. AUTHORIZATION FRAMEWORK — PAYMENT & TRANSACTION TIERS

## 3.1 Transaction Authorization Tiers

Authorization requirements are calibrated to transaction risk. Higher-value or higher-risk actions require stronger authentication. This tiered approach meets NIST AAL requirements and creates a proportionate, court-defensible authorization record.

| Tier | Transaction Type                                                    | Value Range              | Authorization Required                                                 |
|------|---------------------------------------------------------------------|--------------------------|------------------------------------------------------------------------|
| 1    | <b>Browse, search, messaging</b>                                    | No financial value       | Platform login (biometric or PIN)                                      |
| 2    | <b>ATL wallet top-up; fee payment; rental deposit</b>               | < AED 50,000             | Face ID + device confirmation (AAL2)                                   |
| 3    | <b>Property offer submission; MOU signing; IP-Share acquisition</b> | AED 50,000 – AED 500,000 | Face ID + device + in-app confirmation code (AAL2+)                    |
| 4    | <b>Property sale settlement; DLD</b>                                | > AED 500,000            | Face ID + device + 6-digit PIN + SMS OTP to registered number (AAL2++) |

|   |                                                                                                     |           |                                                                                         |
|---|-----------------------------------------------------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------|
|   | transfer instruction;<br>large IP-Share<br>acquisition                                              |           |                                                                                         |
| 5 | Legal representation<br>authorization;<br>contractor selection<br>(fragmented); court<br>submission | Any value | Face ID + PIN + dual authentication +<br>ATLAS Compliance Officer counter-<br>signature |

## IV. COURT-ADMISSIBLE EVIDENCE STRUCTURE

### 4.1 The ATLAS Evidence Chain

Every authorized action on the ATLAS Platform generates an immutable, timestamped evidence chain. This chain is designed to satisfy UAE Federal Law No. 10 of 1992 (Law of Evidence), Article 17-20 requirements for electronic evidence admissibility, and to withstand cross-examination in both UAE civil and commercial courts.

| Evidence Component                  | Technical & Legal Specification                                                                                                                                                                                            |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Biometric Authentication Log</b> | Timestamp (UTC + UAE timezone), device ID, Face ID match result (pass/fail + confidence score), liveness detection result, ISO/IEC 30107-3 certification reference. Stored encrypted; SHA-256 hash recorded on blockchain. |
| <b>Session Token Record</b>         | JWT session token ID, creation timestamp, expiry timestamp, device fingerprint, IP address, geolocation (country/city level), user account reference. Immutable database record + blockchain hash.                         |
| <b>Action Record</b>                | Specific action taken (e.g., 'MOU Signed', 'Escrow Instruction Issued', 'IP-Share Acquired'), action timestamp, transaction ID, counterparty reference, document version hash (SHA-256 of signed document).                |
| <b>Document Hash</b>                | Every signed document is SHA-256 hashed at the moment of biometric signing. Hash stored on blockchain. The document itself and its hash are both retained — any subsequent alteration of the document is detectable.       |
| <b>Blockchain Timestamp</b>         | Merkle tree entry on the ATLAS blockchain layer. Transaction hash, block number, block timestamp. Third-party verifiable — exportable as PDF certificate for court submission.                                             |
| <b>Audit Trail Export</b>           | Full audit trail exportable as: (i) signed PDF with ATLAS official seal; (ii) JSON data package with blockchain verification hashes; (iii) notarised print copy available within 5 business days for court use.            |

# V. LEGAL REPRESENTATION, INTEREST REPRESENTATION & FRAGMENTED CONTRACTOR SELECTION

## 5.1 Legal Representation Authorization

Users may authorize a third party (lawyer, agent, or representative) to act on their behalf for specific Platform transactions. Legal representation authorization requires the highest authentication tier (Tier 5) and generates a platform-issued Power of Attorney reference that is legally equivalent to a notarized PoA for Platform-specific actions.

- Representation authorization is action-specific — the scope of authority is explicitly defined and cannot be unilaterally expanded by the authorized party.
- Representation is time-limited — expiry date is set at the time of authorization and cannot be extended without re-authentication by the principal user.
- Every action taken by a representative is biometrically authenticated under the representative's own Face ID — creating a dual-trace evidence chain (principal authorization + representative action).
- Platform records the authorization grant, the scope, the representative's identity, and every action taken under the authorization — forming a complete representation audit trail.
- Revocation of representation is immediate and requires only Tier 2 authentication by the principal user — no representative consent is required for revocation.

## 5.2 Fragmented Contractor Selection Framework

The ATLAS Platform supports a structured, traceable contractor selection process for property-related services (maintenance, renovation, fit-out, professional services). Fragmented selection — where different contractors are selected for different components of a single project — is fully supported through the following framework:

| Stage                         | Process                                                                                                                                                                                          |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scope Definition              | User defines service scope, budget per component, timeline, and mandatory qualifications (licences, certifications) for each contractor category.                                                |
| Contractor Verification       | All contractors on the ATLAS platform are pre-verified: trade licence, DED registration, insurance certificate, and past performance rating. User selects from verified pool only.               |
| Fragmented Selection          | User selects individual contractors per service component. Each selection is Face ID authorized (Tier 2–3 per contract value). System generates a multi-party service agreement automatically.   |
| Payment Escrow per Contractor | Each contractor's payment is held in a separate escrow sub-account. Funds released only upon user confirmation of milestone completion, authenticated by Face ID.                                |
| Performance Record            | Contractor performance is recorded on the ATLAS platform — ratings, milestone records, and payment history are retained as part of the property's lifecycle record.                              |
| Dispute Resolution            | Disputes with contractors follow the ATLAS dispute resolution protocol — platform arbitration panel has access to the complete authenticated contractor selection and payment trail as evidence. |

---

**Disclaimer:** The authorization and verification framework described in this Policy is continuously updated to reflect technological advances, legal developments, and regulatory guidance. Users are notified of material changes with 30 days' advance notice. ATLAS provides technical audit trail extracts to UAE courts and regulatory authorities upon receipt of a valid court order or regulatory request.