ACS SECURITY SYSTEM

LICENSE SERVER WORKFLOW & MECHANISM

1.Overview

This document outlines the **end-to-end licensing architecture** for ACS.

The design ensures that every license is:

- Bound to a specific machine
- Validated across multiple trust layers
- Centrally controlled
- Secure against tampering and duplication

2.Architectural Principles

The licensing system operates on **three independent trust layers**:

1. Client hardware identity
2. Organization-side license server and database
3. Client-side registry secret key

A license is valid **only when all three layers match**.

3.Workflow

Step 1 – Client Installation & Fingerprinting

During ACS installation, the system collects:

- BIOS Serial
- Disk Serial
- MAC Address
- Machine ID
- Machine Fingerprint
- Product UUID

These uniquely identify the system.

Step 2 – Installation Key Generation

A unique installation key is generated and stored in:
HKEY_LOCAL_MACHINE\SOFTWARE\AcsSecurity

This key:

- Is never exposed to the user
- Acts as a hidden validation factor
- Prevents license cloning

Step 3 – License Request Submission
The client sends collected data to the license server.
The server stores it in:

- **client_lic_request_info** (Pending State)

Step 4 – License Generation (Server Side)
The license server generates a license using:

- Client hardware data
- Stored request information
- Installation key

Configured parameters:

- Client hardware data
- Stored request information
- Installation key

The final record is stored in:

- **client** table

Step 5 – Distribution & Activation
When the license is imported to the client:

ACS validates:

- Hardware identifiers
- Registry installation key
- Server-side license data

If all checks pass:

- License activates
- ACS becomes operational

If any check fails:
License is rejected
System access is restricted

4.Workflow

- Renewal does not alter machine binding

Only configurable parameters change:

- Expiry date

- Modules
- Limits

Full validation remains mandatory.

5.Security Summary

Mechanism	Purpose
Hardware Binding	Prevents license reuse
Registry Secret Key	Prevents tampering
Server-Side Validation	Centralized control
Encrypted License Data	Protects license integrity
Multi-Factor Validation	Strong defence against piracy

6.Business Value

- Eliminates unauthorized deployments
- Ensures predictable revenue control
- Simplifies enterprise-scale rollouts
- Supports audit and compliance needs
- Enables controlled trial and renewal models

6.Executive Conclusion

The ACS licensing architecture delivers a **secure, scalable, and enterprise-grade solution.**

By combining

- Hardware fingerprinting
- Registry-based secrets
- Centralized server validation