

Project Summary

LegitimatelyU was designed to replace password-based authentication with a secure, mobile-first identity layer for apps and websites. The client needed a system that could support biometric login, third-party app integration, and secure backend validation without exposing secrets on the frontend. smartData built a full-stack authentication platform with LU app registration, QR code and unique-ID login flows, web-based approval, secure token exchange, and backend verification using secret keys. The solution also included biometric modalities such as face and voice verification, plus an SDK-oriented integration model for external applications. As a result, the platform creates a single, reusable authentication experience that reduces password dependency, improves login convenience, and strengthens identity assurance across connected systems.

Problem Statement

Traditional username and password authentication is vulnerable to phishing, credential theft, and brute-force attacks. | Users often reuse passwords across multiple services, creating avoidable security exposure and login fatigue. | Different applications typically implement different login methods, which fragments the user experience and slows adoption. | The client needed one reusable authentication layer that could support biometric login and third-party integration. | The system also had to keep secrets server-side and validate responses securely after authentication.

Approach / Solution

smartData built the LU authentication workflow around secure application registration, issuing Client ID, App ID, and Secret Key credentials from the admin portal. | The user-facing flow supports Login with LU through QR code scanning, unique ID entry, or a web-based fallback. | Each request is verified on the backend so the secret key never appears on the frontend. | The solution also supports biometric authentication modes such as face, voice, and iris verification for device-appropriate identity checks. | A reusable SDK-oriented integration model was designed so third-party apps can connect to LU without rebuilding authentication logic.

Technical Challenges

- Challenges

- ★ Supporting multiple biometric methods across different device capabilities.
- ★ Keeping authentication responses secure while integrating third-party apps.
- ★ Making voice verification reliable in noisy real-world conditions.

- How We Solved It

- ★ Built an adaptive enrollment flow that detects available hardware and offers the appropriate biometric option per device.
- ★ Used backend-only verification with unique sessions, secret-key checks, and encrypted transport to prevent frontend exposure.
- ★ Applied VAD, normalization, and ECAPA-TDNN speaker matching with similarity thresholds to improve accuracy.

Learning

Device capability validation should happen early so authentication options match real-world hardware from the start. | Server-side verification must remain the default for every authentication response because frontend trust is never sufficient. | Modular integration design is essential for auth platforms because third-party adoption depends on low-friction onboarding. | Compliance-oriented logging and audit trails should be built in from the first release, not added later.

Screenshots

