# Gatishil Auth v6.5 — Final PRD + Wireframe (Flow of Trust → PIN → Dashboard)

One-liner:  
Seal once, unlock forever. Biometric if available → PIN for everyone → OTP or Magic Link only for new devices or recovery.

## Purpose

One human = one identity spine that feels human everywhere — from a village Android to a Windows desktop with Hello to an iPhone with Face ID. Three doors of trust: Biometric → PIN → OTP/Magic Link.

## Device Capability Awareness

At the Trust Step, the client runs:  
  
if (window.PublicKeyCredential &&  
 await PublicKeyCredential.isUserVerifyingPlatformAuthenticatorAvailable())  
  
If true → device has a built-in authenticator, for example:  
- Apple: Face ID · Touch ID  
- Android: Biometric Prompt · Screen Lock  
- Windows 10/11 (Laptop + Desktop): Windows Hello (Face, Fingerprint, or PIN via TPM chip)  
- Chromebook: Platform Authenticator (Secure Enclave)  
  
If supported → show “Create Passkey 🔐”. The OS then handles Face/Touch/Hello enrollment and stores a hardware-backed credential in its secure chip. On return, the user taps “🖐️ Use Biometric” → instant unlock, no passwords.  
If unsupported → skip passkey button and proceed directly to the 4-digit PIN setup (fallback for all devices).

## Trust Ladder

🔐 Passkey (Biometric): Face ID, Touch ID, Android Prompt, Windows Hello (laptop or desktop)  
🔑 PIN (4 digits): Universal fallback works offline  
✉️ OTP / Magic Link: New device trust or PIN reset

## Functional Flow

1️⃣ New Member  
/join  
- Nepal: verify by OTP (SMS)  
- Abroad: verify by Magic Link (Email)  
/onboard → Name → Roots → Ātma Diśā → Trust Step  
- Detect passkey support → show “Create Passkey 🔐” if available.  
- Always → “Add 4-digit PIN 🔑” + Confirm → Save.  
✅ Toast: “Your voice is now sealed.” → /dashboard.  
  
2️⃣ Returning Member (known device)  
- Biometric (passkey) → success → /dashboard.  
- If biometric unavailable → enter PIN → success.  
- After 5 wrong PINs → soft-lock → OTP/Magic Link → reset PIN → /dashboard.  
  
3️⃣ Returning Member (new or untrusted device)  
- Enter PIN → prompt OTP or Magic Link once to trust device.  
- After verification → device added to trusted\_devices.  
- Next login → PIN only.  
- Optional: “Bind Passkey to this device 🔐” in Security drawer to add Face ID / Hello later.

## Data Storage

webauthn\_credentials: Stores public keys + metadata (Face ID / Hello / Android Prompt)  
account\_secrets: PIN hash (Argon2id + salt + server pepper)  
trusted\_devices: Fingerprint + timestamps + platform info (OS, auth type)

## Security

- PIN never stored raw.  
- 5 failed PINs → delay + CAPTCHA + OTP/Magic Link reset.  
- OTP/Magic Link required only for new-device trust or PIN reset.  
- RP ID locked to gatishilnepal.org (no www).  
- Offline unlock cache syncs when online.

## Microcopy (verbatim)

“Seal your voice to this device 🌿”  
“Add a 4-digit PIN for quick unlock on any device.”  
“On new devices we’ll ask OTP or Magic Link once, then your PIN will work there too.”  
“🖐️ Use Biometric”  
“Forgot PIN → Verify with OTP or Magic Link to reset.”

## Three Flows to Test

1️⃣ Modern Device (Face ID / Android Prompt / Windows Hello Laptop or Desktop)  
Join → OTP/Magic Link → Create Passkey → Add PIN  
→ Relaunch → Biometric Unlock → Works  
→ Disable Biometric → PIN Unlock → Works  
  
2️⃣ Old Phone / Basic Laptop (No Biometric)  
Join → OTP/Magic Link → Add PIN  
→ Login with PIN → OTP/Magic Link once (new device trust)  
→ Next Login → PIN only → Works  
  
3️⃣ Forgot PIN / Recovery  
Login → Wrong PIN × 5 → Soft lock  
→ OTP/Magic Link Verification → Reset PIN → Login → Works

## Final Verdict

Gatishil Auth v6.5 unifies all trust paths: Biometric (Face ID, Touch ID, Android Prompt, Windows Hello laptop/desktop), PIN fallback for any device, and OTP/Magic Link for universal recovery and new-device trust. Every Nepali—whether on a rural phone, Android tablet, Windows desktop, or MacBook—experiences one warm, bank-grade, flicker-free flow of trust.