New NextGate Auth & Onboarding Flow UI (DEPRECATED)

1. Sign Up Flow

Path A: Phone User

```
Enter phone number
       |
       ▼
   Verify OTP
       |
       ▼
  Enter age & name
       |
       ▼
  Pick username
       |
       ▼
 Pick interests (min 3)
       |
       ▼
 Profile setup (optional)
       |
       ▼
   Home Feed □□
(device registered)

── Post-onboarding ──
Soft nudge to add email
(banner only, never blocking)
```

Path B: Email User

```
Enter email address
       |
       ▼
   Verify OTP
       |
       ▼
  Enter age & name
       |
       ▼
  Pick username
       |
       ▼
 Verify phone number ← REQUIRED (Identity)
       |
       ▼
 Pick interests (min 3)
       |
       ▼
 Profile setup (optional)
       |
       ▼
   Home Feed □□
(device registered)
```

Path C: Google / Apple OAuth

```
Tap Google / Apple
       |
       ▼
   OAuth authorize
       |
       ▼
  Enter age & name
  (pre-filled from OAuth)
       |
       ▼
  Pick username
```

```
  (suggestions from name)
       |
       ▼
  Verify phone number ← REQUIRED (Identity)
       |
       ▼
  Pick interests (min 3)
       |
       ▼
  Profile setup (optional)
   (profile pic pre-filled)
       |
       ▼
    Home Feed □□
(device registered)
```

---

2. Onboarding Steps Detail

Step Summary

#	Step	Applies To	Endpoint
0	OTP / OAuth entry	All	`/auth/start` + `/auth/verify` or `/auth/login/oauth`
1	Age & name	All	`/auth/onboarding/age`
2	Username	All	`/auth/onboarding/username`
3	Contact verify (PHONE)	Email + OAuth only	`/auth/onboarding/contact/initiate` + `/contact/verify`
4	Interests	All	`/auth/onboarding/interests`
5	Profile	All	`/auth/onboarding/profile`

Contact Verification Rule

Signup Method	Required Contact	Reason
Phone	~~Email~~ (optional, post-onboarding)	Phone = real identity, M-Pesa already linked

Signup Method	Required Contact	Reason
Email	Phone (blocking)	Needed for M-Pesa payments
Google / Apple	Phone (blocking)	OAuth gives email, phone still required for payments

Onboarding Step Sequence

Phone user:

```
INITIATED → OTP_VERIFIED → AGE_VERIFIED → USERNAME_SET → INTERESTS_SELECTED →
PROFILE_COMPLETED → COMPLETED
```

Email / OAuth user:

```
INITIATED → OTP_VERIFIED → AGE_VERIFIED → USERNAME_SET → CONTACT_VERIFIED → INTERESTS_SELECTED
→ PROFILE_COMPLETED → COMPLETED
```

Token Expiry

Token	Expiry	Purpose
`onboardingToken`	7 days	Active onboarding flow, resets each step
`onboardingRefreshToken`	30 days	Safety net if token expires mid-flow
`accessToken`	Configured	Normal app access
`refreshToken`	Configured	Access token rotation

---

3. Contact Verification — Inline UX (3 states, 1 page)

```
STATE A — Input

┌──────────────────────────────────────┐
│  □□Add your phone number             │
│                                      │
│  Your email j••••@g••••.com □        │
│                                      │
```

```
│  We need your phone for:              │
│  • Offline notifications              │
│  • Account security & recovery        │
│                                       │
│  Phone: [+255_____________]           │
│  [Send Code →]                        │
└───────────────────────────────────────┘


STATE B — OTP Input

┌───────────────────────────────────────┐
│  Enter code sent to ••• ••• ••50      │
│                                       │
│  [_] [_] [_] [_] [_] [_]              │
│                                       │
│  [Edit number]  Resend (60s)          │
└───────────────────────────────────────┘


STATE C — Edit (tapping [Edit number] transforms inline)

┌───────────────────────────────────────┐
│  New number: [+255_____________]      │
│  [Send new code →]    [Cancel]        │
└───────────────────────────────────────┘
```

> Previous OTP invalidated immediately on edit. No page navigation — single page, three inline states.

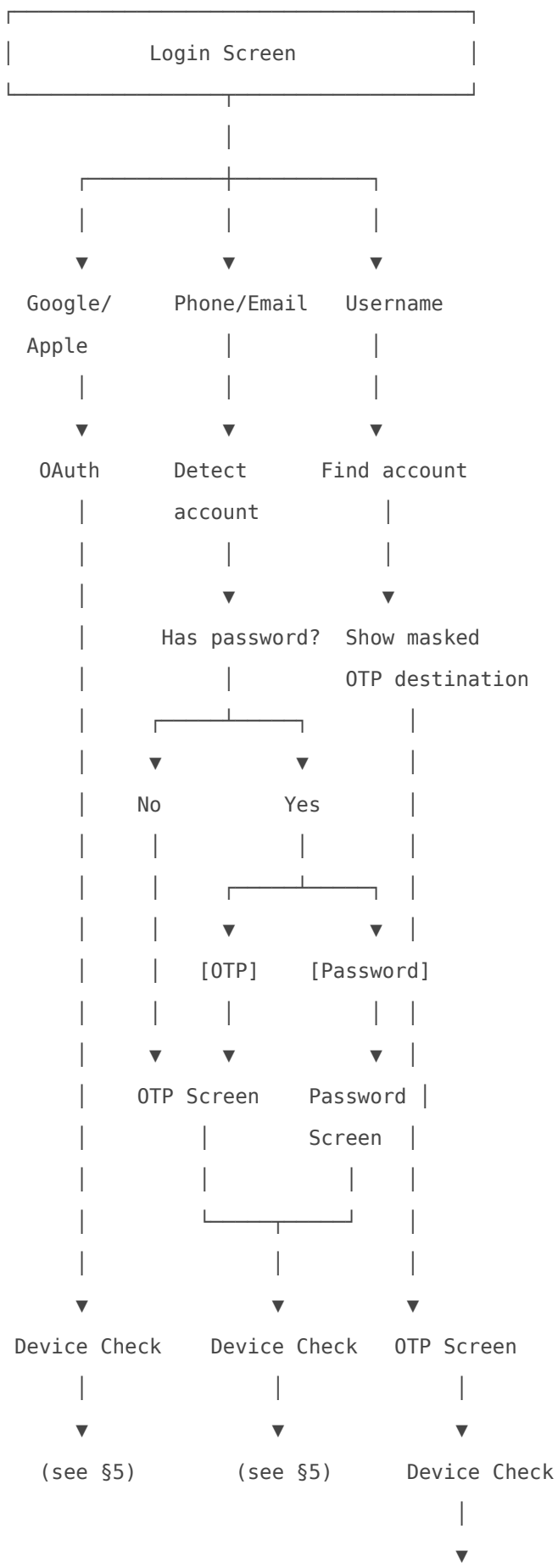
---

4. Login Flow

Identifier Detection

Input pattern	Detected as
Starts with `+`	Phone
Contains `@` + domain	Email
Otherwise	Username

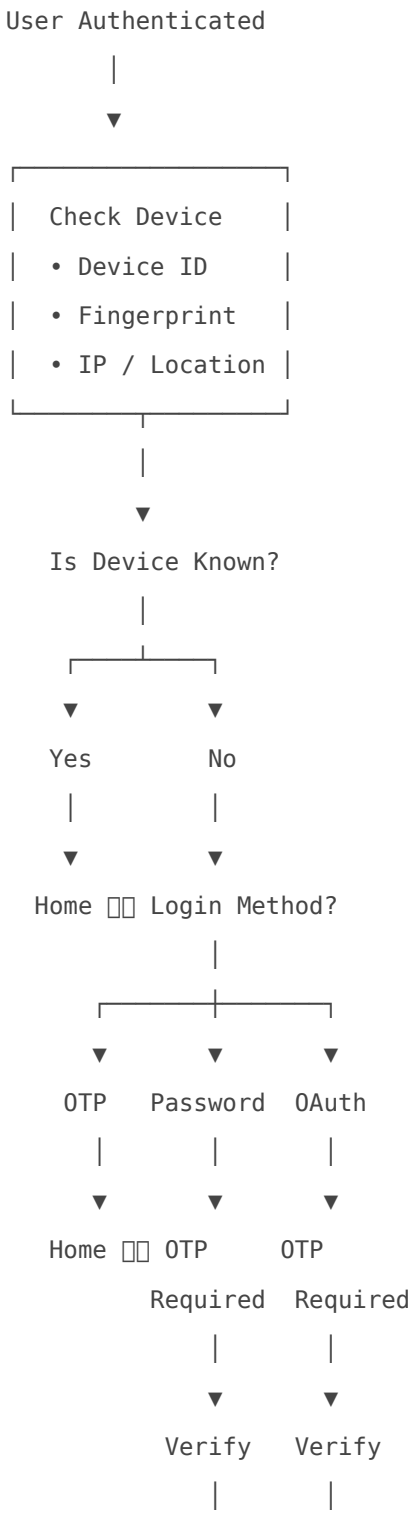
Complete Login Flow



```
                                (see §5)
```

5. Device Trust Check

After Authentication



```
          ▼      ▼
        Register Device
          │
          ▼
        Home □□
```

Device Trust Rules

Login Method	New Device Action	Reason
OTP	None	OTP = already verified
Password	Require OTP	Password could be stolen
OAuth	Require OTP	Token could be compromised

---

6. Risk Scoring

Signal	Low Risk	High Risk
Location	Same country	New country
Device	Similar OS	Different OS
IP	Normal	VPN / Proxy
Account	Active	Dormant
Time	Normal hours	Unusual hours

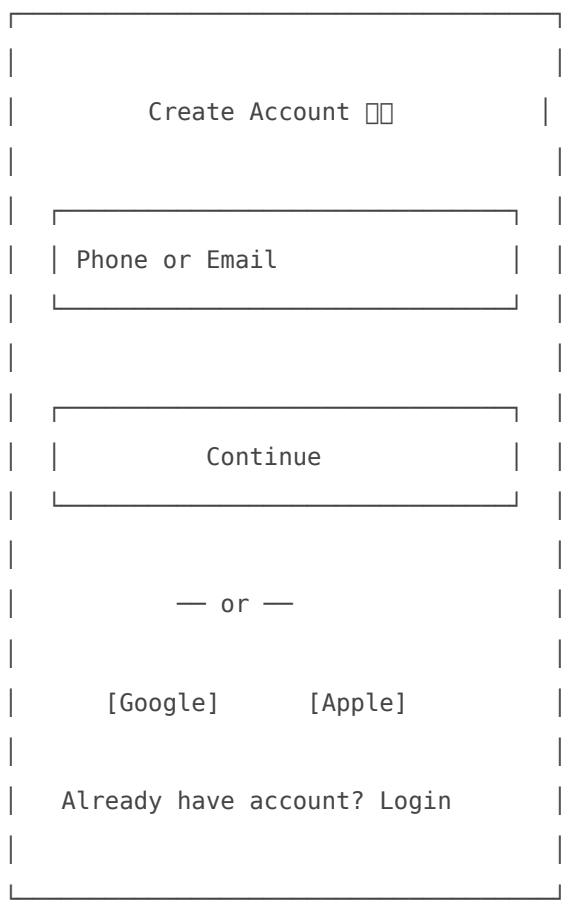
Action by Risk

```
Risk Score
    │
    ├── Low Risk  ──► Soft verify (email link, approve from known device)
    │
    └── High Risk ──► Phone OTP required
```

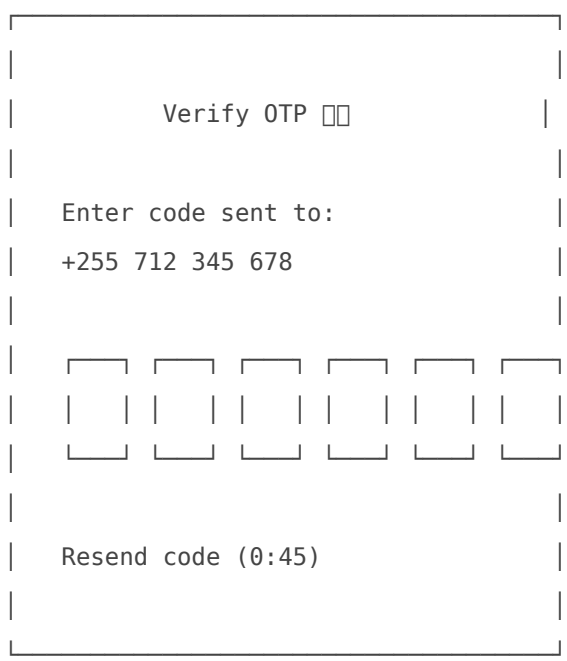
---

7. UI Screens

Sign Up Screen



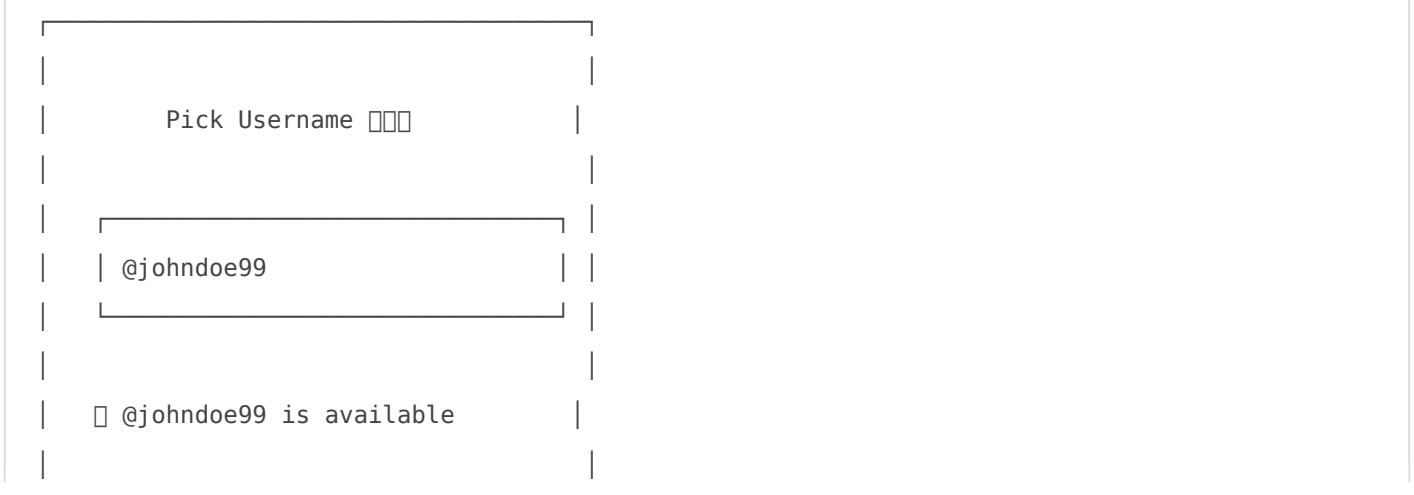
OTP Verification Screen



Age & Name Screen

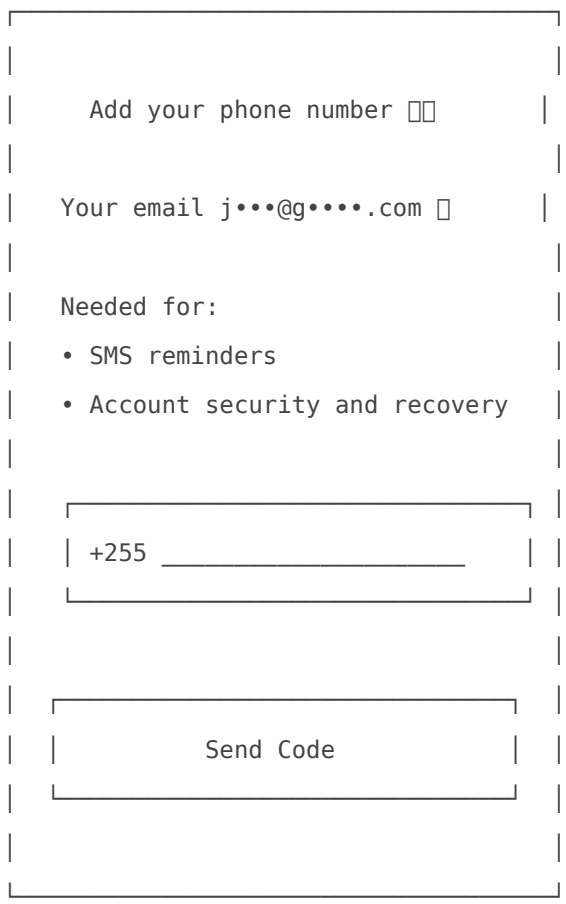


Username Screen

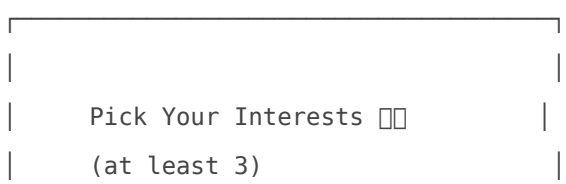


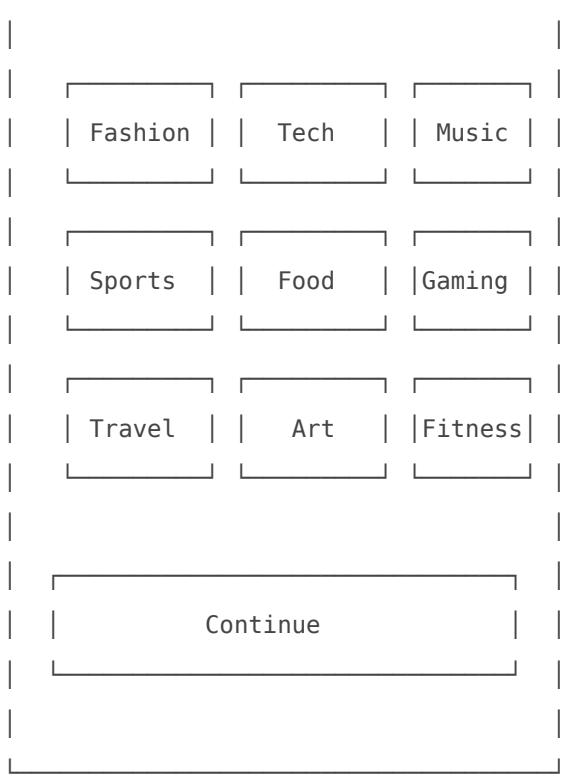


Contact Verification Screen (Email/OAuth users only)

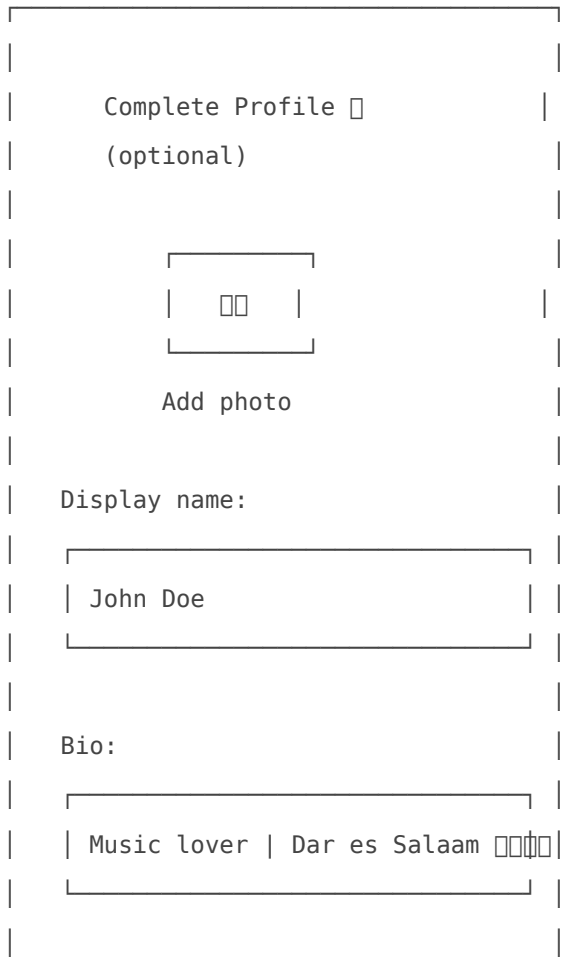


Interests Screen



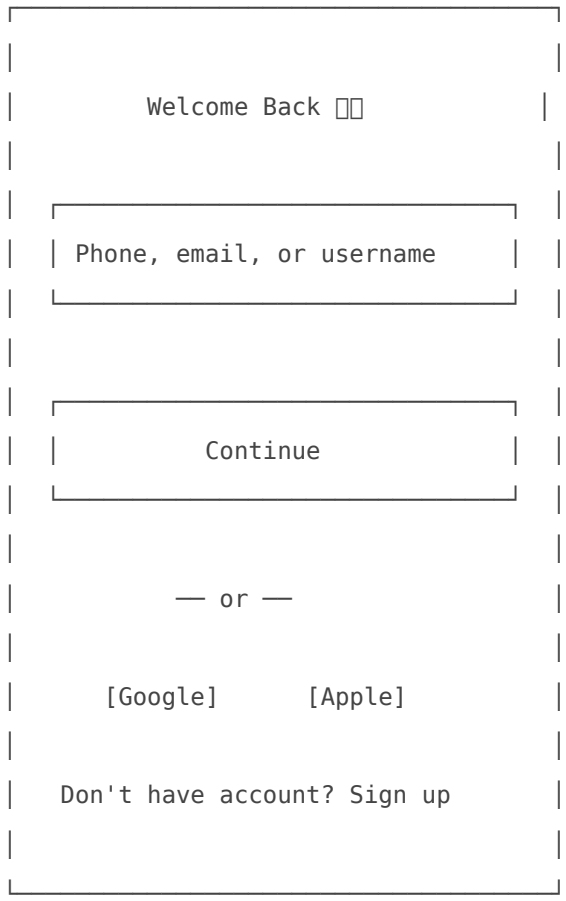


Profile Setup Screen

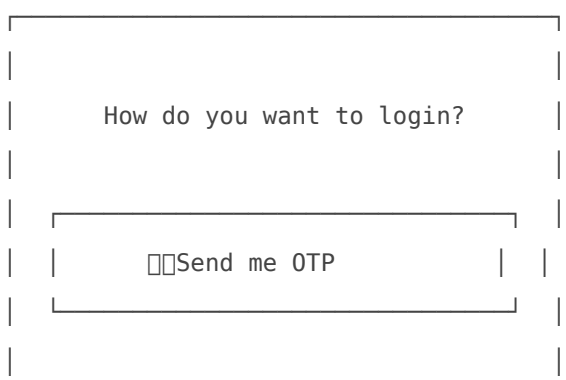


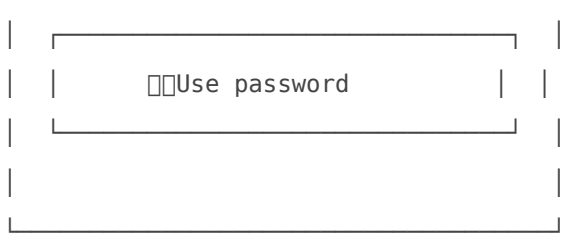


Login Screen

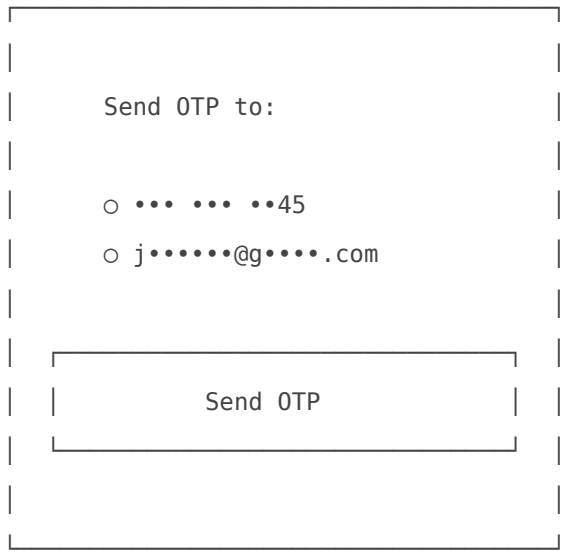


Login Method Choice (if password exists)





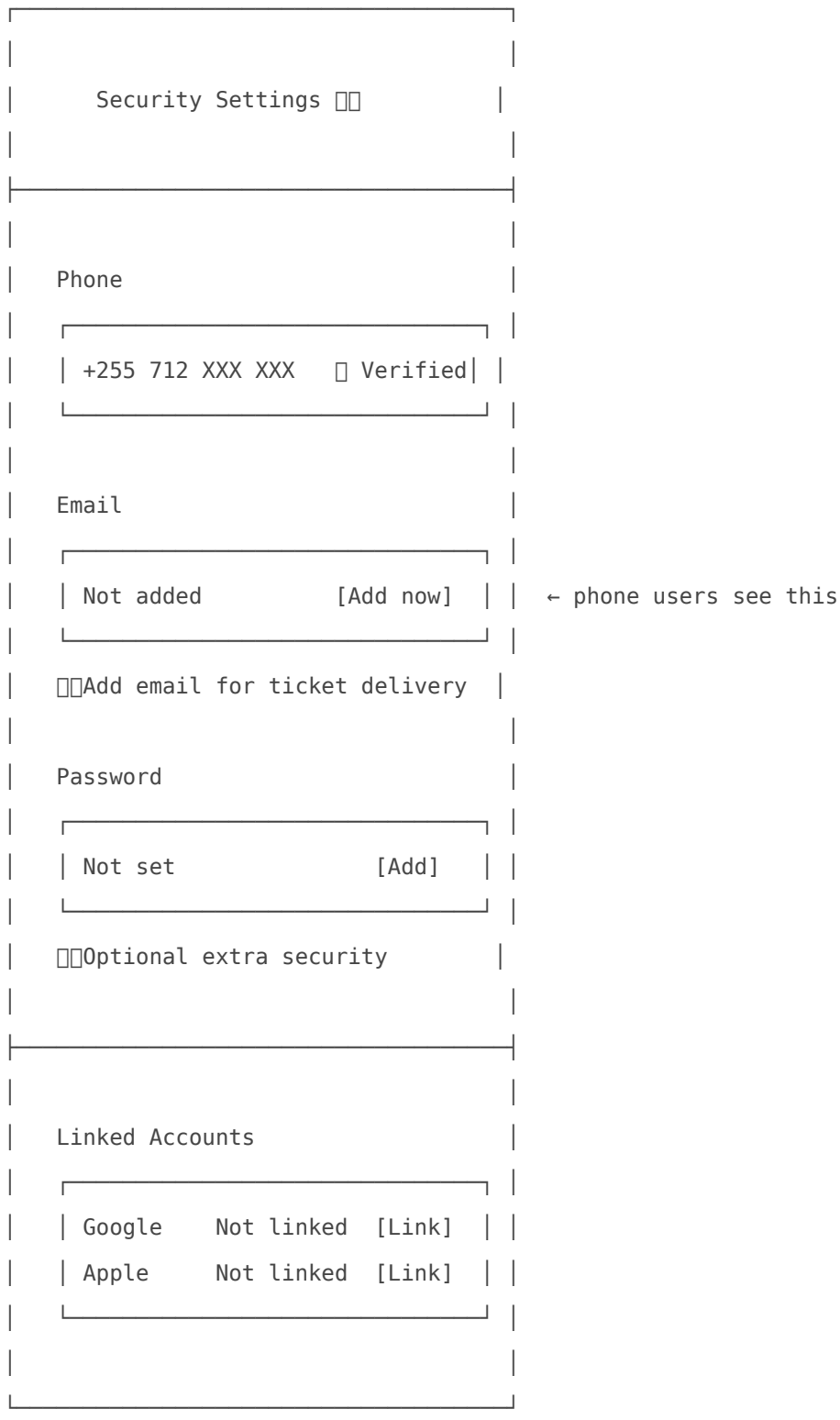
OTP Destination Choice (username login)



New Device Detected



8. Security Settings (Post-onboarding)



9. Summary

Sign Up

Path	Steps
Phone	OTP → Age → Username → Interests → Profile → Home
Email	OTP → Age → Username → **Verify Phone** → Interests → Profile → Home
OAuth	Authorize → Age → Username → **Verify Phone** → Interests → Profile → Home

Login

Has Password?	Options
No	OTP only
Yes	Choose: OTP or Password

Device Verification

Login Method	New Device Action
OTP	None (OTP = verification)
Password	OTP required
OAuth	OTP required

Post-Onboarding Nudges (Phone users)

Feature	Requires Email?	Behaviour
Browse feed	No	Free
Buy ticket	No	Free
Receive ticket via email	Yes	Nudge to add email
Account recovery	Yes	Nudge to add email

Revision #7
Created 11 January 2026 19:39:35 by Admin Qbit
Updated 3 April 2026 10:39:46 by Admin Qbit