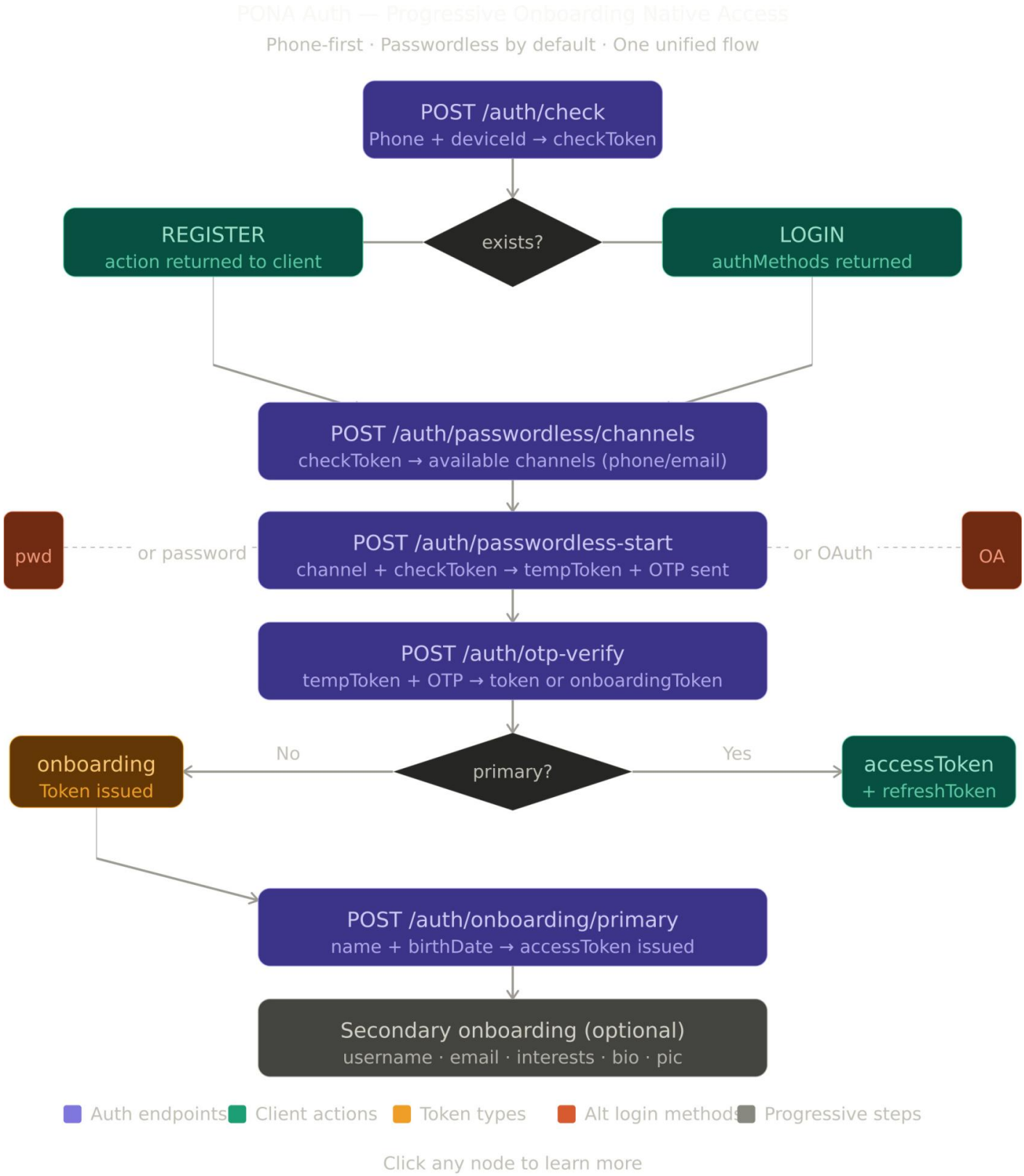
NextGate — PONA Auth Flow V3 (Progressive · Onboarding · Native · Access)

> Version 3.0 — The Complete Authentication Specification

```
Phone-first. Passwordless by default.
One flow. No walls. Trust earned progressively.
```

Philosophy

- **One entry point** — phone number only, always
- **One auth system** — no separate lite or hard auth flows
- **Passwordless by default** — password is an optional enhancement set later
- **Progressive onboarding** — primary is mandatory, secondary collected only when a resource needs it
- **One token type** — access token carries onboarding flags
- **Persistent identity** — device remembers who you are, you never type your number twice
- **Channel choice** — passwordless users pick where they receive their OTP



Token Types

Token	Lifespan	Purpose	Issued At

`checkToken`	5 mins	Signed phone carrier — binds all auth actions to one account	`/auth/check`
`tempToken`	10 mins	OTP handshake only	`/auth/start`, `/onboarding/email/initiate`
`onboardingToken`	7 days	Primary flow only — unlocks name and age steps only	After OTP verified, primary incomplete
`accessToken`	1hr (no password) / 7 days (with password)	Full session, carries onboarding flags	After primary complete
`refreshToken`	30 days	Silent refresh, password users only, rotated on use	After password login

---

What "Primary Complete" Means

Three requirements. All three done before access token is issued. No skip. No cancel.

```
□  Phone verified via OTP
□  First name + Last name set
□  Date of birth set (age calculated → account tier assigned)
```

Account Tiers — Set at Age Step

Age	Tier	What It Means
Under 13	Blocked	Account deleted. Phone blocklisted. Cannot return until 13th birthday.
13 — 17	Restricted	Age-restricted content hidden. Some commerce limited.
18+	Full	No restrictions.

Onboarding Flags (Inside Access Token)

Derived from actual account data. No separate database column needed.

Flag	Means
`primaryComplete`	Phone verified + name set + date of birth set
`username`	Real username chosen — not a system temp one
`email`	Email submitted AND verified via OTP
`profilePic`	At least one profile picture uploaded
`interests`	At least 3 interests selected
`bio`	Bio text written

Access Token Shape

```
{
  "sub": "su_uuid",
  "flags": {
    "primaryComplete": true,
    "username": false,
    "email": false,
    "profilePic": false,
    "interests": false,
    "bio": false
  },
  "exp": "2026-04-01T12:00:00Z"
}
```

Resource Permission Matrix

Feature	Needs Primary	Needs Secondary
Browse events / listings	No auth	—
React / like		nothing extra
Buy ticket or product		nothing extra
Share listing		nothing extra
Comment publicly		`username`
Follow someone		`username`
Send a message		`username`
Create an event		`username` + `email`

Feature	Needs Primary	Needs Secondary
Open a shop		`username` + `email`
Sell a product		`username` + `email`
Withdraw money		`username` + `email` + `profilePic`
Age-restricted content	must be 18+	nothing extra

Secondary Field Priority Order

Backend returns missing fields one at a time in this order. User never sees all missing fields at once.

```
1 — username      (needed for almost all social features)
2 — email         (needed for commerce and trust)
3 — profilePic    (needed for high-trust actions)
4 — bio           (rarely hard-required)
5 — interests     (feed personalization, almost never hard-required)
```

Auth Method Validation

Every auth endpoint validates the user has the method they are trying to use.

Endpoint	Validation
`/auth/login/password`	Account must have password set
`/auth/login/oauth` Google	Google must be linked to this account
`/auth/login/oauth` Apple	Apple must be linked to this account
`/auth/password/forgot/initiate`	Account must have password set
`/auth/passwordless/channels`	Always allowed
`/auth/start` OTP	Always allowed — passwordless available to everyone

OTP Channel Selection

Passwordless users with email set can choose where to receive their OTP. Frontend never passes the raw email or phone — only the channel type enum.

Channel Availability Rules

Channel	Available When
`PHONE`	Always — phone is primary, always verified
`EMAIL`	Only when email is set AND verified on the account

Action Codes — Complete Reference

Action Code	What Frontend Does
`REGISTER`	New user — show registration intro
`CONTINUE_ONBOARDING`	Returning user, primary incomplete — resume
`LOGIN`	Account ready — show auth method options
`RESTART_AUTH`	Token expired — back to phone entry
`SELECT_CHANNEL`	Multiple OTP channels — show picker
`PROCEED_TO_OTP`	Single channel only — skip picker, go straight to OTP
`USE_OTP`	Wrong auth method chosen — switch to OTP
`RETRY_OTP`	Wrong OTP — error on same screen
`RESEND_OTP`	OTP expired — activate resend
`WAIT`	Rate limited — show countdown
`ACCOUNT_BLOCKED`	Under 13 — show blocked screen
`COLLECT_USERNAME`	Username needed
`COLLECT_EMAIL`	Email needed — submit then OTP verify
`COLLECT_PROFILE_PIC`	Profile picture needed
`COLLECT_INTERESTS`	Interests needed
`COLLECT_BIO`	Bio needed
`PROCEED`	All steps done — retry original action

Response Shapes

Success

```
{
  "success": true,
  "message": "Human readable message",
  "action": "NEXT_ACTION_OR_NULL",
  "data": { }
}
```

Error — HTTP 422

```
{
  "success": false,
  "message": "Human readable message",
  "action": "NEXT_ACTION_CODE",
  "context": "what_user_was_trying_to_do",
  "data": { }
}
```

Response Examples

/auth/check — New User

```
{
  "success": true,
  "message": "Phone number not registered",
  "action": "REGISTER",
  "data": { "exists": false, "checkToken": null }
}
```

/auth/check — Existing User Ready

```
{
  "success": true,
  "message": "Welcome back",
```

```
  "action": "LOGIN",
  "data": {
    "exists": true,
    "checkToken": "eyJ...",
    "primaryComplete": true,
    "maskedPhone": "••• ••• ••78",
    "authMethods": {
      "passwordless": true,
      "password": true,
      "google": true,
      "apple": false
    }
  }
}
```


/auth/check — Primary Incomplete


```
{
  "success": true,
  "message": "Continue setting up your account",
  "action": "CONTINUE_ONBOARDING",
  "data": {
    "exists": true,
    "checkToken": "eyJ...",
    "primaryComplete": false,
    "maskedPhone": "••• ••• ••78"
  }
}
```


/auth/passwordless/channels — Multiple Channels


```
{
  "success": true,
  "message": "Choose where to receive your code",
  "action": "SELECT_CHANNEL",
  "data": {
    "channels": [
```

```
      { "type": "PHONE", "masked": "••• ••• ••78", "isPrimary": true },
      { "type": "EMAIL", "masked": "j••••@g••••.com", "isPrimary": false }
    ]
  }
}
```

/auth/passwordless/channels — Single Channel Only

```
{
  "success": true,
  "message": "Sending code to your phone",
  "action": "PROCEED_TO_OTP",
  "data": {
    "channels": [
      { "type": "PHONE", "masked": "••• ••• ••78", "isPrimary": true }
    ]
  }
}
```

/auth/start — OTP Sent

```
{
  "success": true,
  "message": "Verification code sent",
  "action": null,
  "data": {
    "tempToken": "eyJ...",
    "maskedDestination": "••• ••• ••78",
    "channel": "PHONE",
    "expiresInSeconds": 120,
    "resendAvailableAfterSeconds": 60
  }
}
```

/auth/verify — Primary Incomplete

```
{
  "success": true,
  "message": "Phone verified. Let us set up your account.",
  "action": "COLLECT_PRIMARY",
  "data": {
    "onboardingToken": "eyJ...",
    "nextStep": "name"
  }
}
```


/auth/verify — Primary Already Complete


```
{
  "success": true,
  "message": "Welcome back!",
  "action": null,
  "data": {
    "accessToken": "eyJ...",
    "onboarding": {
      "primaryComplete": true,
      "username": true,
      "email": false,
      "profilePic": false,
      "interests": false,
      "bio": false
    }
  }
}
```


/auth/onboarding/age — Blocked Underage


```
{
  "success": false,
  "message": "You must be at least 13 years old to use NextGate",
  "action": "ACCOUNT_BLOCKED",
  "context": "underage",
  "data": { "unblockDate": "2027-06-15" }
}
```

/auth/onboarding/age — Primary Complete


```
{
  "success": true,
  "message": "Welcome to NextGate!",
  "action": null,
  "data": {
    "accessToken": "eyJ...",
    "accountTier": "FULL",
    "onboarding": {
      "primaryComplete": true,
      "username": false,
      "email": false,
      "profilePic": false,
      "interests": false,
      "bio": false
    }
  }
}
```


OTP Wrong


```
{
  "success": false,
  "message": "Incorrect OTP code",
  "action": "RETRY_OTP",
  "context": "otp_verify",
  "data": { "attemptsRemaining": 2 }
}
```


OTP Expired


```
{
  "success": false,
  "message": "OTP has expired",
  "action": "RESEND_OTP",
  "context": "otp_expired",
  "data": { "resendAvailable": true, "resendCooldownSeconds": 0 }
```

```
}
```

Rate Limited

```
{
  "success": false,
  "message": "Too many attempts. Please wait.",
  "action": "WAIT",
  "context": "rate_limited",
  "data": { "retryAfterSeconds": 120 }
}
```

Wrong Auth Method

```
{
  "success": false,
  "message": "This account does not use password login",
  "action": "USE_OTP",
  "context": "password_login",
  "data": { "availableMethods": ["passwordless", "google"] }
}
```

Secondary Gate — Multiple Missing

```
{
  "success": false,
  "message": "A couple of things needed before you can create events",
  "action": "COLLECT_USERNAME",
  "context": "create_event",
  "data": {
    "currentMissing": "username",
    "allMissing": ["username", "email"],
    "stepsRemaining": 2
  }
}
```

Secondary Step Done — Next Signalled

```
{
  "success": true,
  "message": "Username set. One more step.",
  "action": "COLLECT_EMAIL",
  "context": "create_event",
  "data": {
    "accessToken": "eyJ...",
    "nextMissing": "email",
    "stepsRemaining": 1,
    "onboarding": {
      "primaryComplete": true,
      "username": true,
      "email": false,
      "profilePic": false,
      "interests": false,
      "bio": false
    }
  }
}
```


All Secondary Done — Proceed


```
{
  "success": true,
  "message": "All done. Creating your event now.",
  "action": "PROCEED",
  "context": "create_event",
  "data": {
    "accessToken": "eyJ...",
    "stepsRemaining": 0,
    "onboarding": {
      "primaryComplete": true,
      "username": true,
      "email": true,
      "profilePic": false,
      "interests": false,
      "bio": false
    }
  }
```

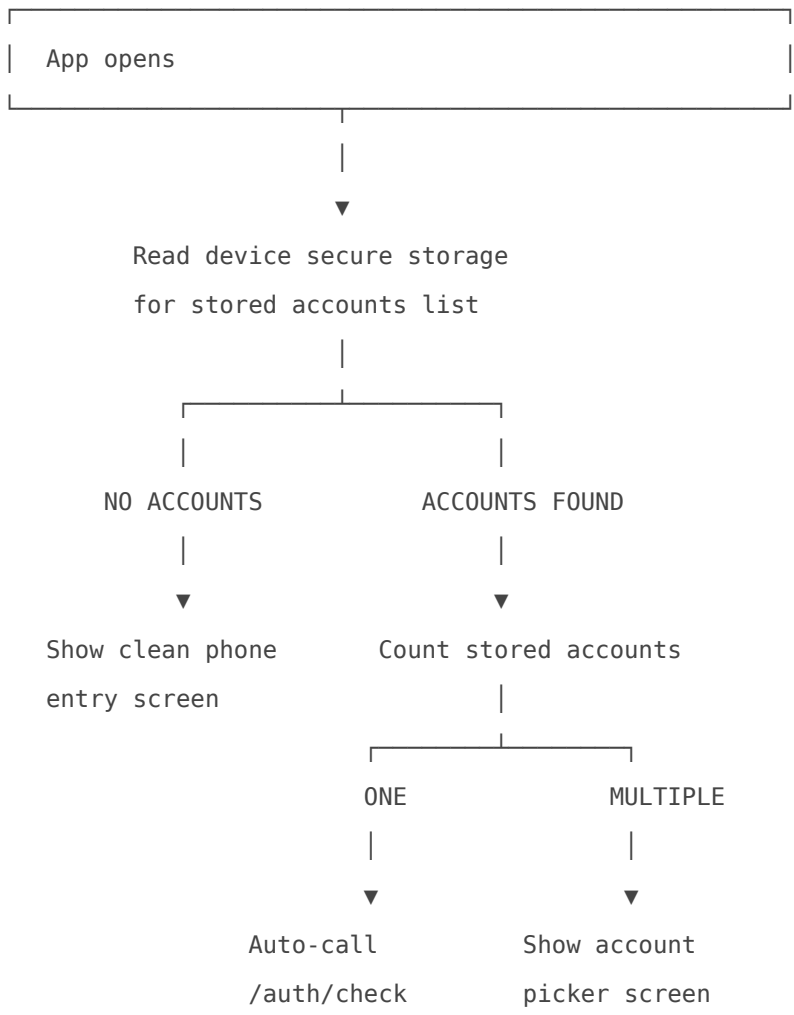
```
}
```

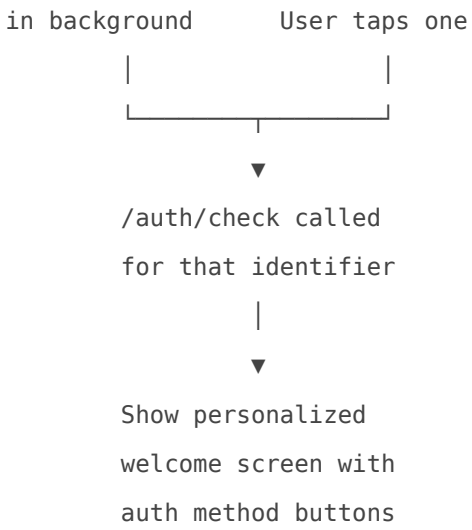
Forgot Password — Reset Complete

```
{
  "success": true,
  "message": "Password updated. All other sessions signed out.",
  "action": null,
  "data": { "accessToken": "eyJ..." }
}
```

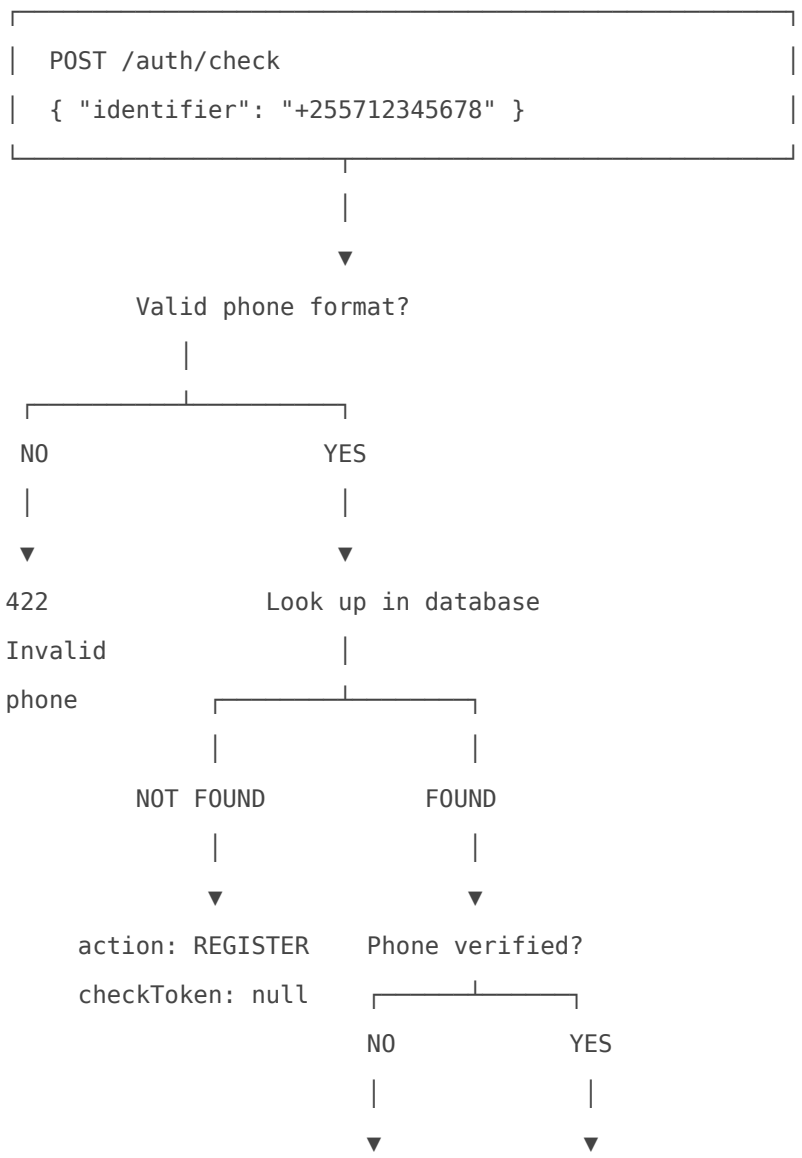
Flow Diagrams

FLOW 1 — App Open with Stored Accounts





FLOW 2 — Auth Check (Entry Point)



```
                Release phone  Primary complete?
                from orphan    ┌──────┴──────┐
                action: REGISTER NO          YES
                              │              │
                              ▼              ▼
                       action:        action: LOGIN
                       CONTINUE_      authMethods
                       ONBOARDING     returned
                              │              │
                              └──────┬───────┘
                                     ▼
                            checkToken issued
                            containing { identifier }
                            stored to device on success
```

FLOW 3 — New User Registration

```
action: REGISTER from /auth/check
.........................................
┌──────────────────────────────────────────────────────┐
│  POST /auth/start                                    │
│  { "checkToken": "eyJ...", "channel": "PHONE" }      │
└──────────────────────┬───────────────────────────────┘
                       │
                       ▼
          Phone extracted from checkToken
          Partial account created
          OTP sent via SMS
          tempToken issued
                       │
                       ▼
┌──────────────────────────────────────────────────────┐
│  POST /auth/verify                                   │
│  { "tempToken": "eyJ...", "otp": "123456" }          │
└──────────────────────┬───────────────────────────────┘
                       │
                       ▼
           Phone verified
```

```
          Primary incomplete
          ONBOARDING TOKEN issued
          App locked to primary screens
                        |
                 ┌──────┴──────┐
                 ▼             ▼
  POST /auth/              POST /auth/
  onboarding/name          onboarding/age
  { firstName,             { birthDate }
    lastName }                   |
       |                         ▼
       ▼                 Under 13? → BLOCKED
  New onboarding           13-17 → RESTRICTED
  token returned           18+   → FULL
  Continue to age                |
                                 ▼
                       PRIMARY COMPLETE
                       ACCESS TOKEN issued
                       Identifier + name + avatar
                       saved to device storage
                       User lands on feed ✓
```

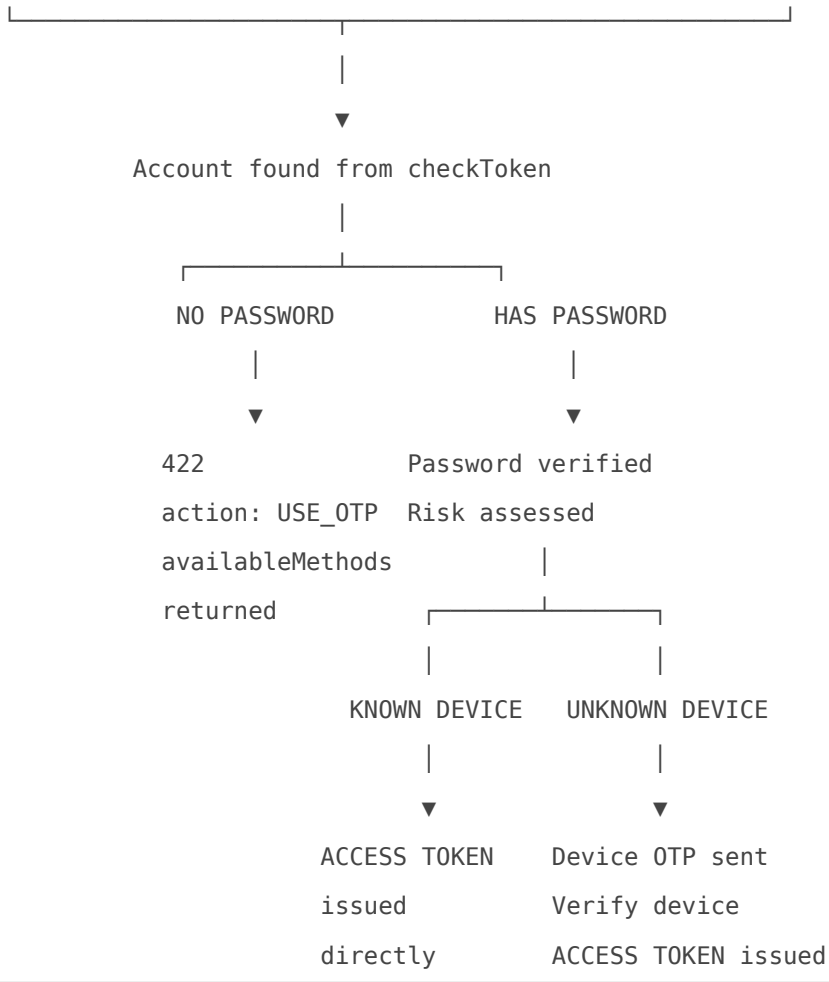
FLOW 4 — Existing User, Passwordless Login

```
action: LOGIN, authMethods.passwordless: true
User picks OTP option
.......................................
┌──────────────────────────────────────────────────┐
│  POST /auth/passwordless/channels                │
│  { "checkToken": "eyJ..." }                      │
└──────────────────────┬───────────────────────────┘
                       |
                       ▼
          Backend checks account channels
                       |
                ┌──────┴──────┐
                |             |
       ONE CHANNEL          MULTIPLE CHANNELS
```

```
      (phone only)          (phone + email)
            |                      |
            ▼                      ▼
     action:               action: SELECT_CHANNEL
     PROCEED_TO_OTP        Show channel picker
     Skip picker            User picks PHONE or EMAIL
            |                      |
            └──────────┬───────────┘
                       ▼
┌──────────────────────────────────────────────────────┐
│  POST /auth/start                                    │
│  { "checkToken": "eyJ...", "channel": "PHONE" }      │
│  or { "checkToken": "eyJ...", "channel": "EMAIL" }   │
└──────────────────────┬───────────────────────────────┘
                       │
                       ▼
          Backend extracts actual phone or email
          internally from account
          Sends OTP to chosen channel
          tempToken issued
                       │
                       ▼
POST /auth/verify { tempToken, otp }
                       │
                       ▼
           OTP valid. Primary complete.
           ACCESS TOKEN issued.
           Device storage entry updated.
           User lands on feed ✓
```

FLOW 5 — Existing User, Password Login

```
action: LOGIN, authMethods.password: true
User picks password option
.........................................
┌──────────────────────────────────────────────────────┐
│  POST /auth/login/password                           │
│  { "checkToken": "eyJ...", "password": "..." }       │
```



FLOW 6 — OAuth Login

```
action: LOGIN, authMethods.google: true
User picks Google
.........................................
┌──────────────────────────────────────────────────────┐
│  POST /auth/login/oauth                              │
│  { "checkToken": "eyJ...",                           │
│    "provider": "GOOGLE", "code": "..." }             │
└──────────────────────┬───────────────────────────────┘
                       │
                       ▼
         Account found from checkToken
         Google linked to account?
                       │
            ┌──────────┴──────────┐
            NO                    YES
```

```
        |                   |
        ▼                   ▼
  422               Google identity confirmed
  action: USE_OTP   Profile data pre-filled
  availableMethods  from Google
  returned                  |
                    Primary complete?
                    ┌───────┴────────┐
                    NO               YES
                    |                |
                    ▼                ▼
              ONBOARDING TOKEN   ACCESS TOKEN
              collect age        issued ✓
```

FLOW 7 — Forgot Password

```
Only shown when authMethods.password: true
.........................................
┌──────────────────────────────────────────────────────┐
│  POST /auth/password/forgot/initiate                 │
│  { "checkToken": "eyJ..." }                          │
└──────────────────────┬───────────────────────────────┘
                       |
                       ▼
        Account has password?
           |
  ┌────────┴──────────┐
 NO                  YES
 |                    |
 ▼                    ▼
422              OTP sent to phone
action: USE_OTP  tempToken issued
                       |
                       ▼
POST /auth/password/forgot/verify-otp
{ tempToken, otp }
                       |
                       ▼
```

```
            OTP verified
            resetToken issued (10 mins, single use)
                        |
                        ▼
POST /auth/password/forgot/reset
{ resetToken, newPassword, confirmPassword }
                        |
                        ▼
            Password updated
            All other sessions revoked
            ACCESS TOKEN issued
            User logged in ✓
```

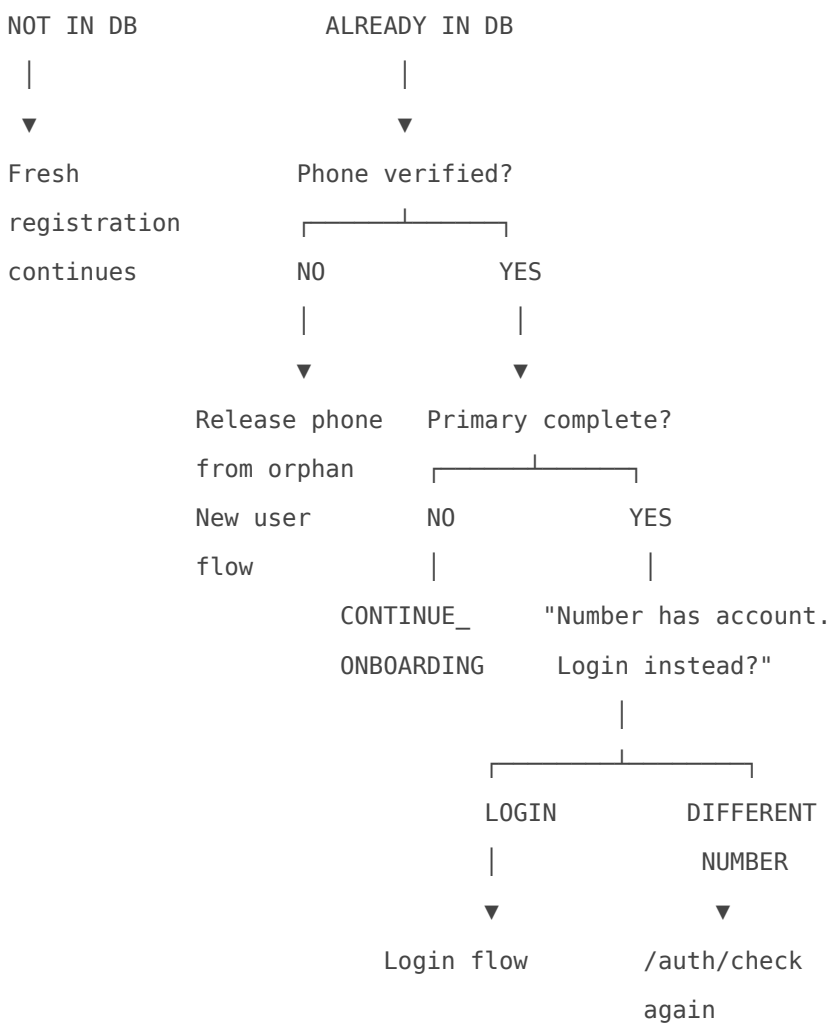
FLOW 8 — Secondary Onboarding (Progressive)

```
User tries to create an event
Needs: username + email
username: false ← first missing
email:    false
.........................................
422 from resource guard
action: COLLECT_USERNAME
allMissing: ["username", "email"]
stepsRemaining: 2
.........................................
Frontend: "2 steps — Step 1 of 2"

POST /onboarding/username
Bearer <accessToken>
{ "username": "joshsakweli" }
        |
        ▼
Username saved
New accessToken issued
action: COLLECT_EMAIL
stepsRemaining: 1
.........................................
```

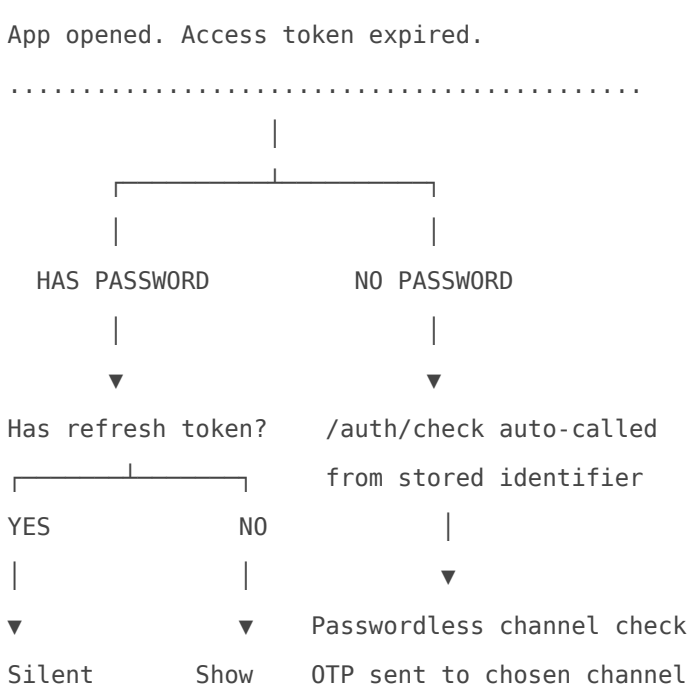
```
Frontend: "Step 2 of 2 — Add email"

POST /onboarding/email/initiate
Bearer <accessToken>
{ "email": "josh@qbitspark.com" }
        |
        ▼
OTP sent to email
tempToken returned
nextAction: VERIFY_EMAIL
        |
        ▼
POST /onboarding/email/verify
Bearer <accessToken>
{ "tempToken": "eyJ...", "otp": "123456" }
        |
        ▼
Email verified
New accessToken issued
action: PROCEED
stepsRemaining: 0
        |
        ▼
Frontend retries create event
Passes ✓
```

FLOW 9 — Wrong Number, Changing During Registration

```
User typed wrong number
OTP sent. User clicks "Change number"
Before OTP verified — just restart
.........................................

POST /auth/check { correct number }
        |
  ┌─────┴──────────────────┐
  |                        |
```



FLOW 10 — Returning User, Token Expired



```
refresh      login   /auth/verify
ACCESS       screen  Primary complete → ACCESS TOKEN
TOKEN                directly, no onboarding shown ✓
issued ✓
```

Client-Side Persistent Identity

This is a frontend-only feature. Zero backend changes required.

What Gets Stored on Device

```
┌──────────────────────────────────────────────┐
│  Stored after every successful login         │
│                                              │
│  identifier    →  "+255712345678"            │
│  maskedPhone   →  "••• ••• ••78"             │
│  displayName   →  "Joshua Sakweli"           │
│  avatarUrl     →  "https://..."              │
│  lastLoginAt   →  "2026-04-01T10:00:00Z"     │
└──────────────────────────────────────────────┘


NEVER store:
✗  Access tokens
✗  Refresh tokens
✗  Passwords or OTPs
✗  Full unmasked phone number in plain text
```

Storage Location by Platform

Platform	Storage Method
Android	`EncryptedSharedPreferences` — hardware-backed encryption
iOS	`Keychain` — secure enclave
Web	`localStorage` — for non-sensitive display data only, never tokens

Stored Accounts List Rules

```
Maximum 5 accounts stored per device
Sorted by lastLoginAt — most recently used first
Updated after every successful login (name, avatar may change)
If 6th account added → prompt user to remove one first
```

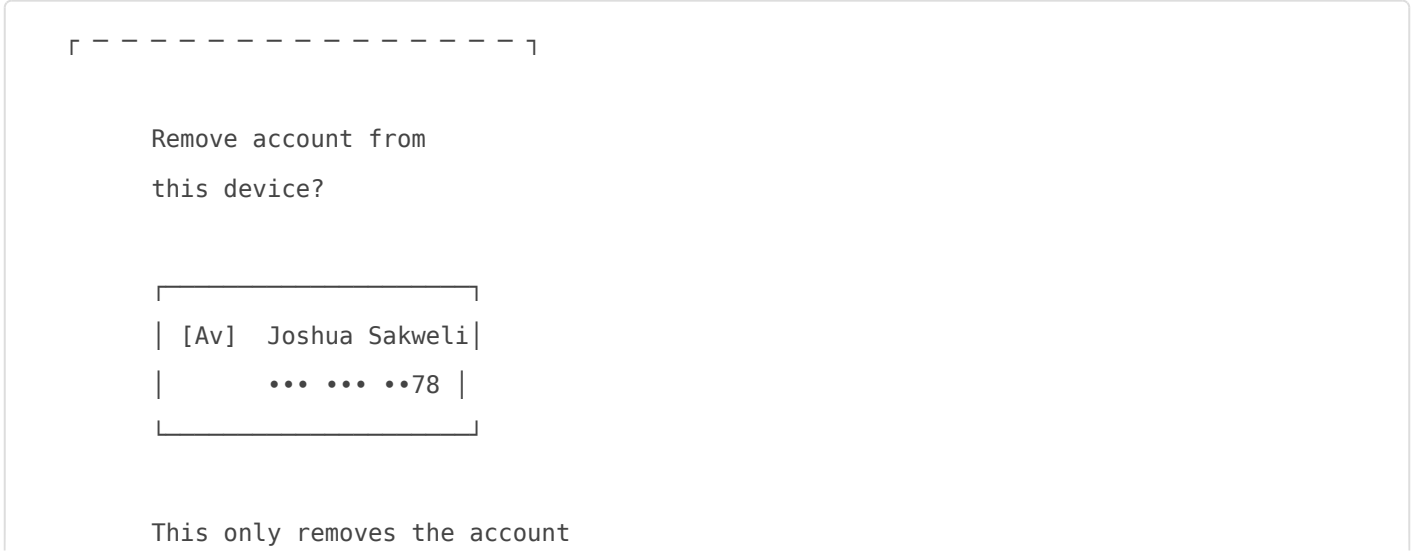
UI Screens (Dotted)

Screen 1 — App Open, One Stored Account

```
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐

      [NextGate Logo]

      ┌──────────────────────┐
      │    [  Avatar  ]      │
      │   Joshua Sakweli     │
      │   ••• ••• ••78       │
      └──────────────────────┘

      ┌──────────────────────┐
      │   Continue with OTP  │  ← primary option
      └──────────────────────┘

      ┌──────────────────────┐
      │   Use Password       │  ← only if password set
      └──────────────────────┘

      ┌──────────────────────┐
      │   G  Continue with   │  ← only if google linked
      │      Google          │
      └──────────────────────┘

      Not you?  Sign in with a different account

└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

Screen 2 — Account Picker (Multiple Stored Accounts)

Screen 3 — Remove Account Confirmation

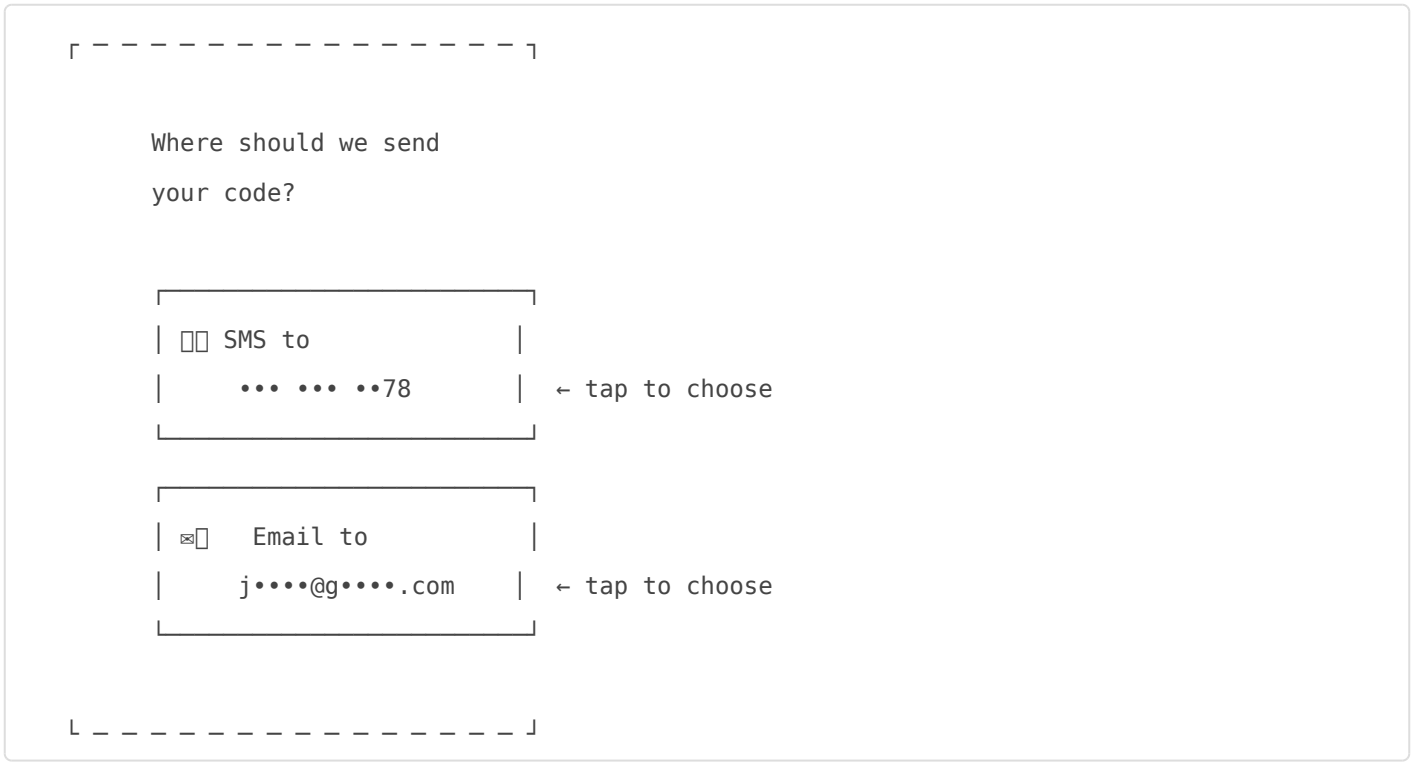


```
        from this device. Your NextGate
        account will not be deleted.

        ┌──────────────────────┐
        │      Remove          │
        └──────────────────────┘

        ┌──────────────────────┐
        │      Cancel          │
        └──────────────────────┘

└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

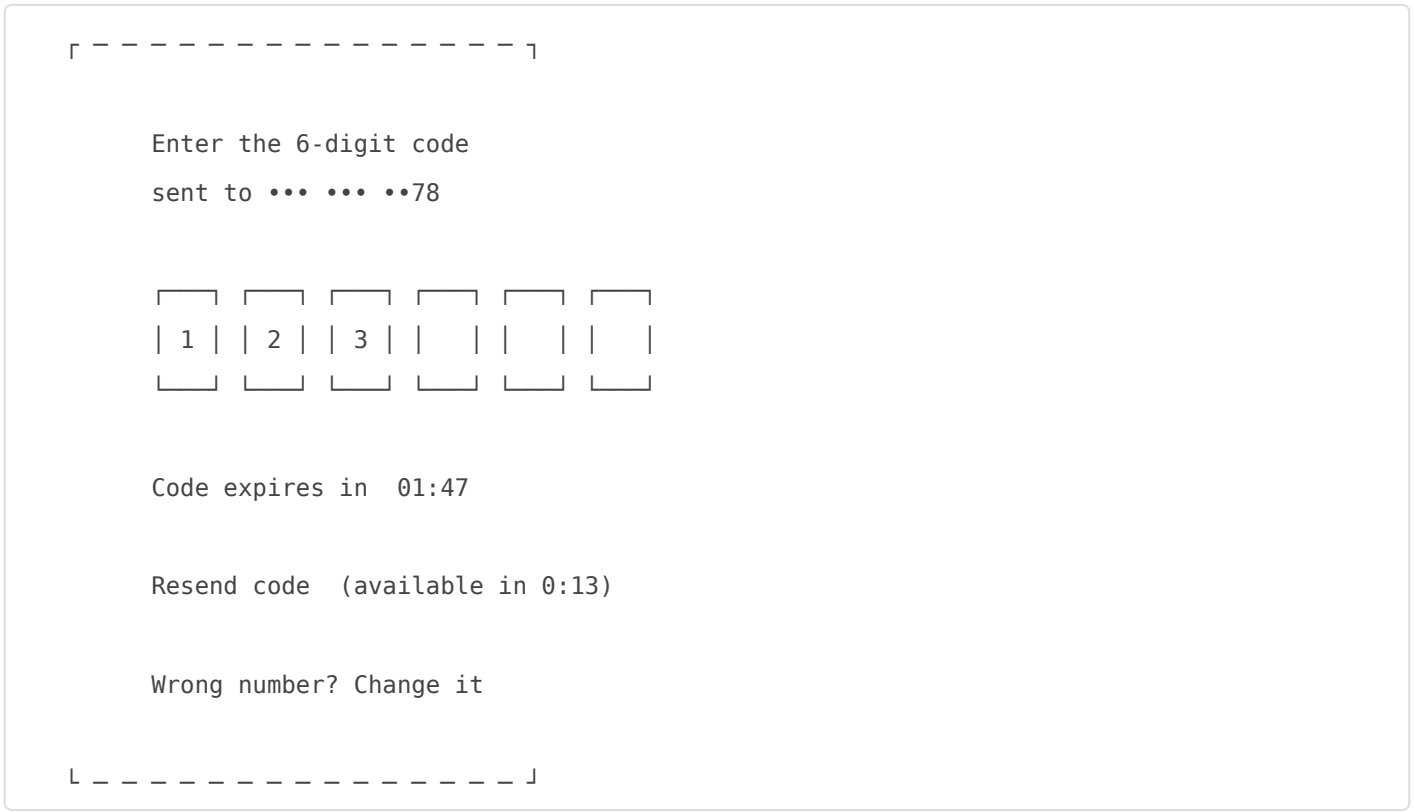
Screen 4 — Fresh Phone Entry (No Stored Account)

```
┌ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┐

        [NextGate Logo]

        Enter your phone number
        to get started

        ┌──────┐  ┌──────────────┐
        │ +255 │  │  7XX XXX XXX  │
        └──────┘  └──────────────┘

        ┌──────────────────────┐
        │      Continue        │
        └──────────────────────┘

        By continuing you agree to our
        Terms of Service and Privacy Policy

└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

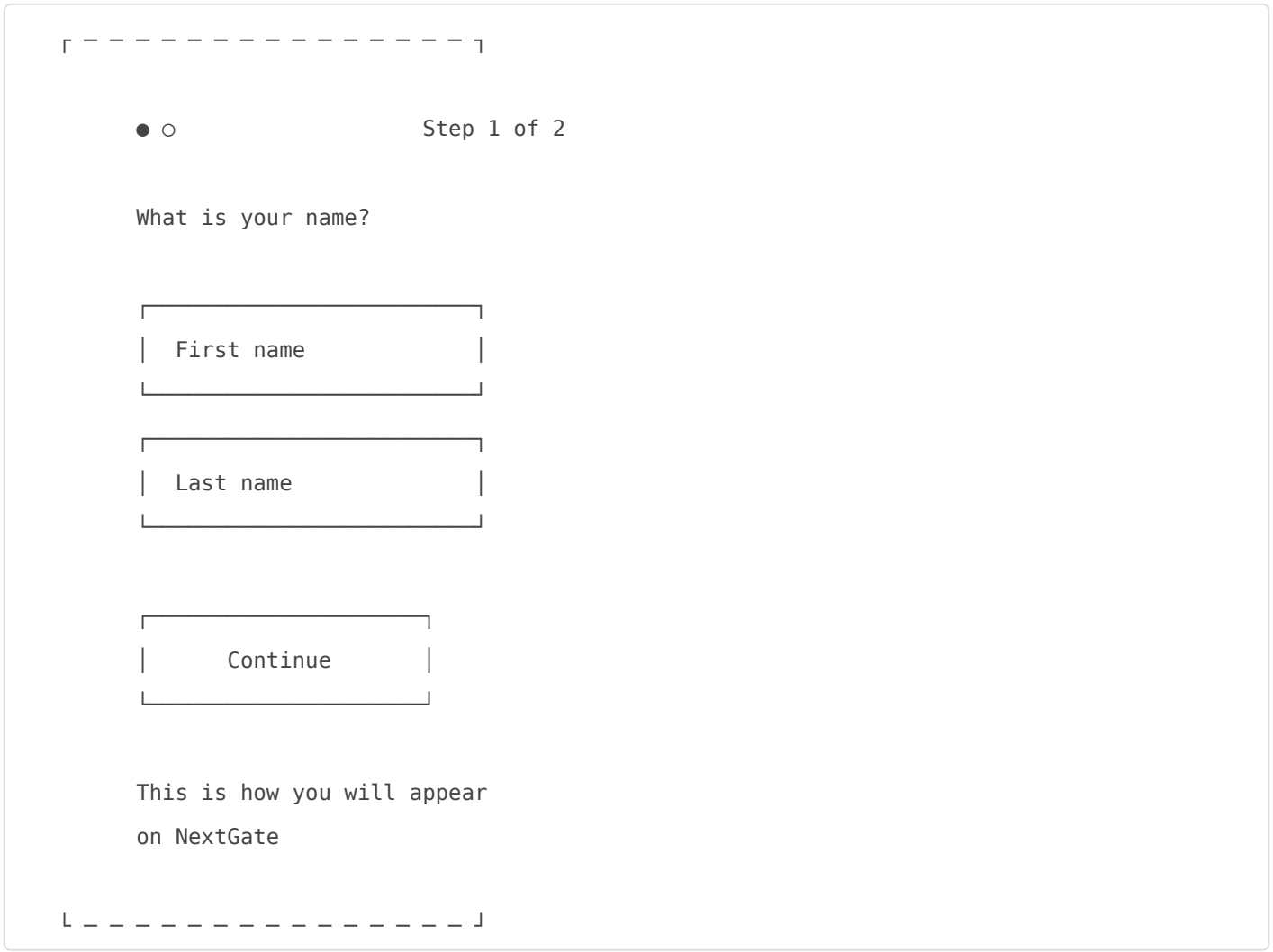
Screen 5 — OTP Channel Picker



Screen 6 — OTP Entry



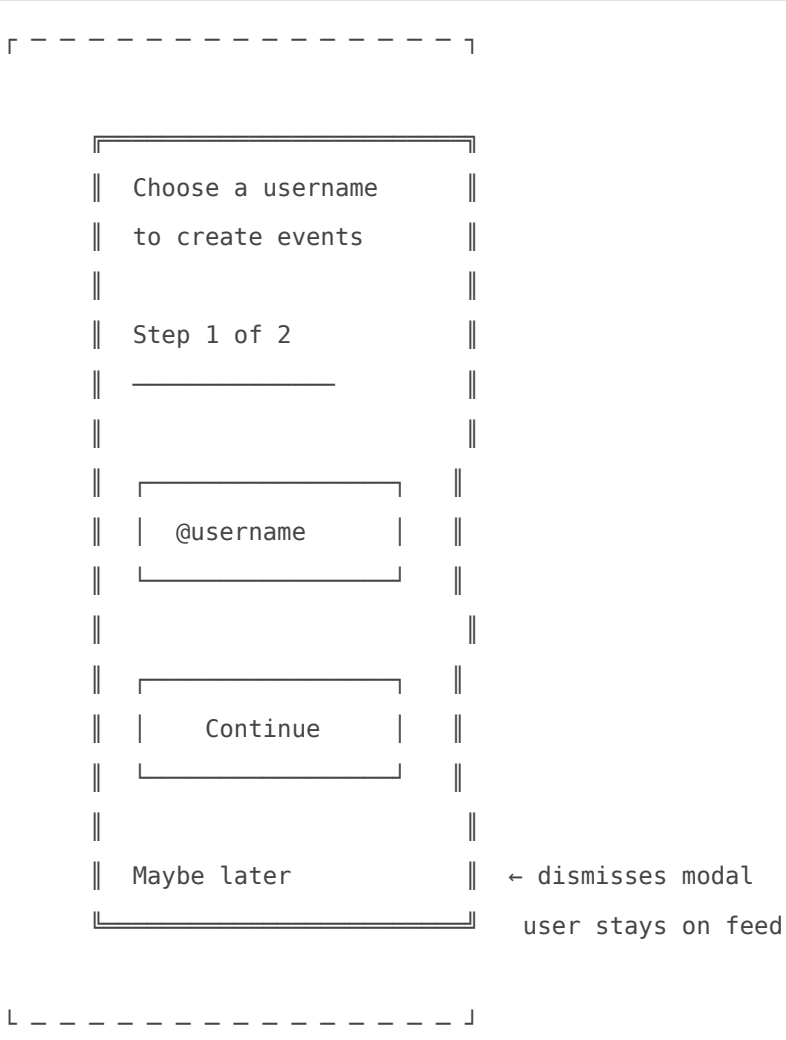
Screen 7 — Primary Onboarding, Name Step



Screen 8 — Primary Onboarding, Age Step

```
      Your age helps us show you
      the right content.
      We never share your birthday.

└ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ┘
```

Screen 9 — Secondary Onboarding Gate (Inline, Not Full Screen)



> Secondary onboarding appears as a **bottom sheet or modal**, not a full page. User can dismiss it and continue browsing. They will be prompted again when they try the same action.

Screen 10 — Forgot Password

Endpoint Reference

Public — No Auth Required

Method	Endpoint	Send	Receive
POST	`/auth/check`	`{ identifier }`	checkToken + exists + authMethods
POST	`/auth/passwordless/channels`	`{ checkToken }`	available channels masked
POST	`/auth/start`	`{ checkToken, channel }`	tempToken
POST	`/auth/verify`	`{ tempToken, otp }`	onboardingToken or accessToken
POST	`/auth/login/password`	`{ checkToken, password }`	accessToken or device flow
POST	`/auth/login/oauth`	`{ checkToken, provider, code }`	accessToken or onboardingToken

Method	Endpoint	Send	Receive
POST	`/auth/resend-otp`	`{ tempToken }`	new tempToken
POST	`/auth/device/verify`	`{ deviceVerificationToken, otp }`	accessToken
POST	`/auth/password/forgot/initiate`	`{ checkToken }`	tempToken
POST	`/auth/password/forgot/verify-otp`	`{ tempToken, otp }`	resetToken
POST	`/auth/password/forgot/reset`	`{ resetToken, newPassword, confirmPassword }`	accessToken

Primary Onboarding — Onboarding Token Required

Method	Endpoint	Send	Receive
POST	`/auth/onboarding/name`	`{ onboardingToken, firstName, lastName }`	new onboardingToken
POST	`/auth/onboarding/age`	`{ onboardingToken, birthDate }`	accessToken

Secondary Onboarding — Access Token Required

Method	Endpoint	Send	Receive
POST	`/onboarding/username`	`{ username }`	new accessToken + next action
POST	`/onboarding/bio`	`{ bio }`	new accessToken + next action
POST	`/onboarding/interests`	`{ interestIds[] }`	new accessToken + next action
POST	`/onboarding/profile-pic`	multipart image	new accessToken + next action
POST	`/onboarding/email/initiate`	`{ email }`	tempToken + nextAction
POST	`/onboarding/email/verify`	`{ tempToken, otp }`	new accessToken + next action

Session Management — Access Token Required

Method	Endpoint	Send	Receive
POST	`/auth/token/refresh`	`{ refreshToken }`	new accessToken + refreshToken
POST	`/auth/token/revoke`	`{ refreshToken }`	success
POST	`/auth/sessions/sign-out`	—	success
GET	`/auth/sessions`	—	active sessions list
DELETE	`/auth/sessions/{id}`	—	success

Client-Side Storage Specification

Storage Keys

```
ng_stored_accounts    →  JSON array of stored account objects
ng_active_identifier  →  identifier of currently active session
```

Stored Account Object

```
{
  "identifier": "+255712345678",
  "maskedPhone": "••• ••• ••78",
  "displayName": "Joshua Sakweli",
  "avatarUrl": "https://cdn.nextgate.app/avatars/...",
  "lastLoginAt": "2026-04-01T10:00:00Z"
}
```

Account Management Rules

Action	What Happens
Successful login	Add or update entry in stored list. Update lastLoginAt, name, avatar.
Normal logout	Keep entry in stored list. User sees welcome back on next visit.
"Forget this device" logout	Remove entry from stored list. Clean phone entry shown next visit.

Action	What Happens
Remove from picker	Remove entry from stored list. Account still exists on server.
Add another account	Login flow, auto-added to list on success.
6th account added	Prompt user to remove one existing entry first.
Account deleted on server	Remove entry from stored list automatically after next failed check.

What to Update After Successful Login

```
After ACCESS TOKEN received:
  → Update displayName from onboarding flags if changed
  → Update avatarUrl if changed
  → Update lastLoginAt to now
  → Sort stored list by lastLoginAt descending
```

What Changes vs What Stays

Being Removed

- Single linear `OnboardingStep` tracking → replaced by independent flags
- `onboardingStep` database column → database migration required
- `isOnboardingComplete()` → replaced by `isPrimaryComplete()`
- Onboarding token for secondary steps → access token handles all of that now
- `refreshOnboardingToken` endpoint → no longer needed
- Email and username as login identifiers → phone only from now on
- Raw identifier passed to `/auth/start` → replaced by `checkToken` + `channel`

Being Added

- `POST /auth/check` — new entry point
- `POST /auth/passwordless/channels` — new channel check endpoint
- `OnboardingFlagResolver` — derives all flags from existing account data
- Resource guard — checks flags, returns next action automatically
- `checkToken` generation in JWT system
- `channel` field on `/auth/start`
- All secondary onboarding endpoints
- `action` and `context` on all responses

- Client-side persistent identity (frontend only, zero backend changes)

Staying Exactly as They Are

- All OTP generation, validation, and rate limiting
- Session creation and management
- Device trust and registration
- Risk assessment and scoring
- Account blocking for underage users and fraud
- Password change and management
- Email and phone account linking (post-login)
- JWT signing infrastructure
- Security filter chain — minor flag reading addition only

Security Notes

- `/auth/check` rate limited — max 10 per IP per minute, max 3 per phone per hour
- `checkToken` single-use — consumed the moment any auth action is taken
- `checkToken` cryptographically binds the phone to every action — identifier cannot be swapped mid-flow
- Frontend never passes raw email or phone after `/auth/check` — channel type enum only
- Orphaned partial accounts cleaned up automatically every night
- Phone collision with verified account — redirected to login, cannot overwrite
- Phone collision with unverified account — released and reassigned via OTP proof
- Primary onboarding — no cancel, no skip, app stays locked until all three steps done
- Underage — account deleted immediately, phone blocklisted, cannot return until 13th birthday
- Forgot password link — never shown unless `authMethods.password: true`
- Wrong auth method — backend validates before doing anything, 422 returned immediately
- Stored accounts on device — only display data stored, never tokens or passwords
- "Forget this device" — clears stored identifier, forces fresh phone entry next visit

---

Revision #4
Created 1 April 2026 00:21:00 by Admin Qbit
Updated 3 April 2026 12:22:53 by Admin Qbit