NextGate Authentication Specification v1.0 (DEPRECATED)

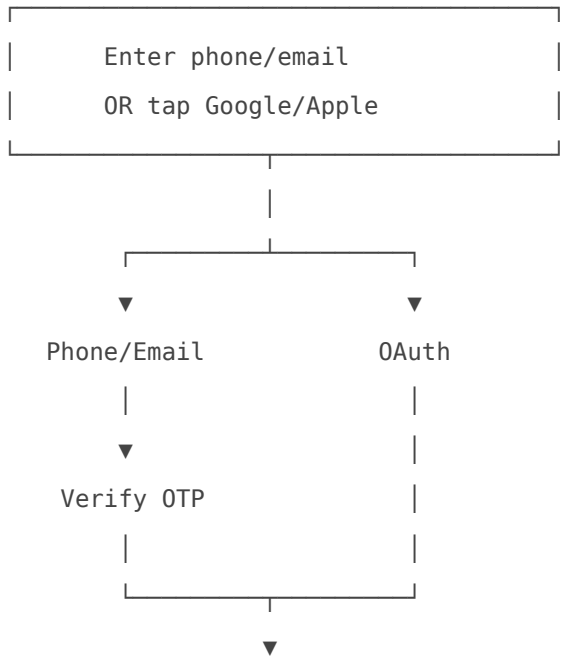
1. Overview

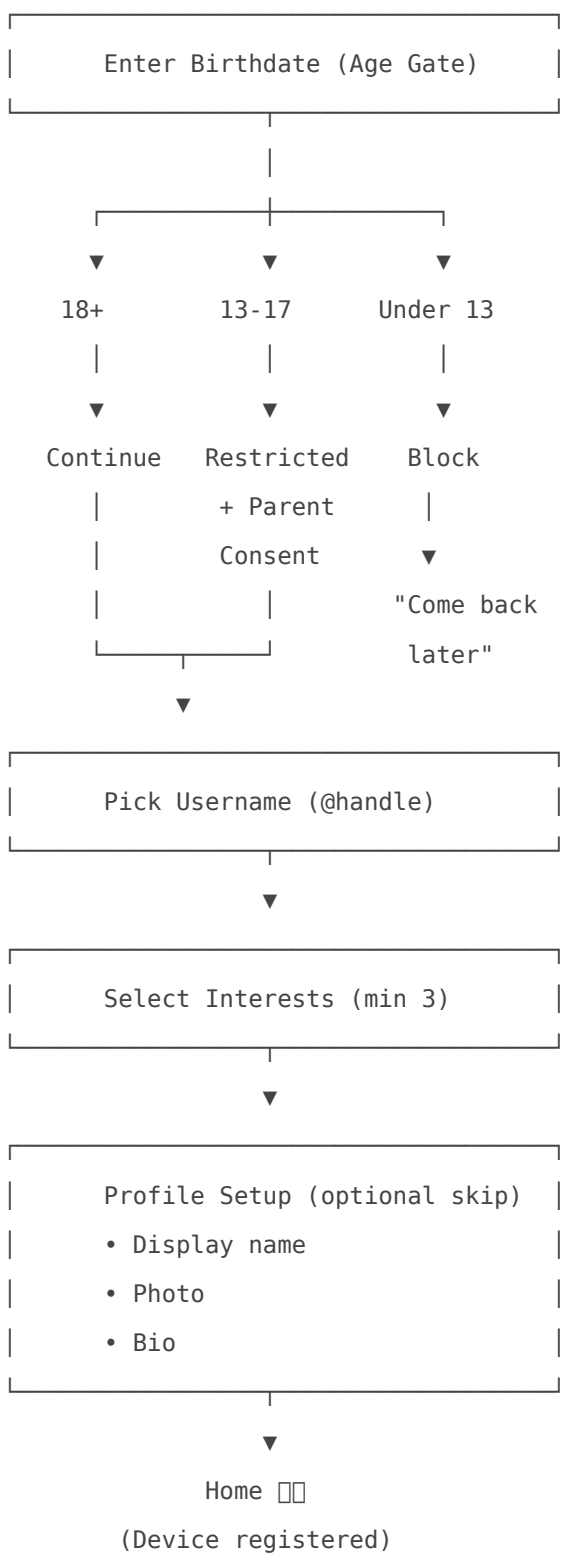
Approach: Passwordless-first, device-trusted, risk-aware authentication.

Principle	Implementation
Passwordless default	OTP-based, password optional (add later in settings)
Device trust	Hardware-bound keys (mobile), fingerprint (web)
Risk-based	Dynamic verification based on risk score
Age-gated	18+ full access, tiered restrictions below

---

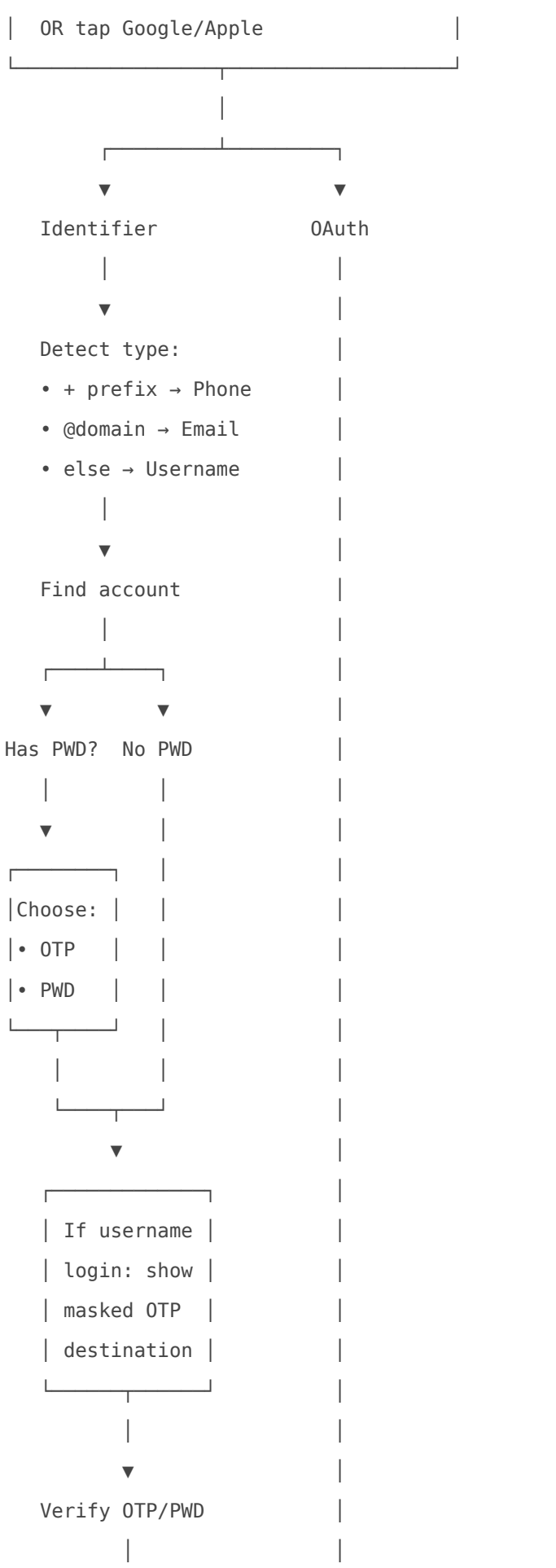
2. Sign Up Flow




Enter Birthdate (Age Gate)
18+
13-17
Under 13
Continue
Restricted
+ Parent
Consent
Block
"Come back
later"
Pick Username (@handle)
Select Interests (min 3)
Profile Setup (optional skip)
• Display name
• Photo
• Bio
Home
(Device registered)

3. Login Flow


Enter phone/email/username


OR tap Google/Apple
Identifier
OAuth
Detect type:
• + prefix → Phone
• @domain → Email
• else → Username
Find account
Has PWD?
No PWD
Choose:
• OTP
• PWD
If username login: show masked OTP destination
Verify OTP/PWD

```
          └──────────┬──────────┘
                     ▼
               Device Check
                     │
          (see section 5)
```

OTP Destination (Username Login)

```
┌──────────────────────────────────────┐
│      Send OTP to:                    │
│                                      │
│      ○ ••• ••• ••45                  │
│      ○ j••••••@g••••.com             │
│                                      │
│      [Send OTP]                      │
└──────────────────────────────────────┘

If only one exists → skip choice, send directly
```

---

4. Login Method Summary

Has Password?	Login Options
No	OTP only (passwordless)
Yes	Choose: OTP or Password

Login Method	New Device Handling
OTP	None needed — OTP is verification
Password	OTP required on new device
OAuth	OTP required on new device

---

5. Device Trust

Platform Strategy

Platform	Method	Trust Level
iOS	Secure Enclave key pair	□□□□□ High
Android	StrongBox/TEE Keystore	□□□□□ High
Web	Fingerprint + session key	□□□ Medium

Mobile Device Registration



Login with Device Verification



```
│    stored public key                │
│    • Valid → trusted device ✅      │
│    • Invalid → block ❌             │
└─────────────────────────────────────┘
```

Why Attacker Fails

```
Attacker has:     ✅ Password, ✅ DeviceId, ✅ Nonce
Attacker needs:   ❌ Private key (locked in victim's hardware)
Result:           ❌ Cannot forge signature → Attack fails
```

---

6. Risk Scoring

Signals & Weights

Signal	Low (0)	Medium	High
Location	Same city	Same country (+10)	New country (+25)
Device	Known (0)	Similar OS (+10)	New OS (+20)
IP	Normal ISP (0)	Different ISP (+10)	VPN/TOR (+30)
Time	Normal hours (0)	Unusual (+10)	2-5 AM (+15)
Failed attempts	None (0)	1-2 (+10)	3+ (+25)
Velocity	Normal (0)	Multiple (+15)	Rapid (+30)
Device signature	Valid (-20)	Missing (+15)	Invalid (+40)

Thresholds & Actions

Score	Risk Level	Action
0-30	◻️ Low	Allow
31-60	◻️ Medium	Soft verify (email link)
61-85	◻️ High	Phone OTP required
86-100	❌ Critical	Block + alert user

Impossible Travel

```
Last login: Dar es Salaam at 10:00 AM
This login: London at 10:30 AM
Distance: 7,500 km in 30 min = impossible

→ +40 points → likely compromised
```

---

7. Age Restriction

Tiers

Age	Access Level
18+	Full access
13-17	Restricted (no purchases, filtered content)
Under 13	Blocked (COPPA)

Blocked User Handling



---

8. Username Rules

Change Limits (Anti-Fraud)

Account Age	Allowed Changes
Day 0 (today)	5 changes
1-30 days	1 per month
1-12 months	1 per month
12+ months	1 per year
SYSTEM accounts	Never

Account Types

Type	Examples	Username Change
NORMAL	Regular users	Limited (above)
SYSTEM	@nextgate, @admin, @support	Never
VERIFIED	@nike, @cocacola	Requires approval

---

9. Session Management

Sign Out Options

Action	What It Does	Requires
Sign out	Current device only	Nothing
Sign out others	All except current	OTP/Password
Sign out all	Everything	OTP/Password

Active Sessions View

```
┌─────────────────────────────────────┐
│ □□iPhone 14 Pro                     │
│    Dar es Salaam • Active now       │
```

```
│    This device                [●]  │
├────────────────────────────────────┤
│ □□Chrome on Windows                │
│    Nairobi • 2 hours ago           │
│                          [Sign out] │
├────────────────────────────────────┤
│ [Sign out other devices]           │
│ [Sign out all devices] ⚠□          │
└────────────────────────────────────┘
```

---

10. Security Settings

```
┌────────────────────────────────────┐
│ Security Settings □□               │
├────────────────────────────────────┤
│ Phone: +255 712 •••456   □ Verified │
│ Email: j••••@email.com   □ Verified │
├────────────────────────────────────┤
│ Password: Not set           [Add]  │
│ □□Optional extra security          │
├────────────────────────────────────┤
│ Linked Accounts:                   │
│ Google: Not linked         [Link]  │
│ Apple: Not linked          [Link]  │
└────────────────────────────────────┘
```

---

11. API Endpoints

Auth - Signup

Endpoint	Purpose
`POST /auth/signup/initiate`	Start signup (phone/email)
`POST /auth/signup/verify-otp`	Verify OTP
`POST /auth/signup/age`	Submit birthdate

Endpoint	Purpose
`POST /auth/signup/username`	Set username
`POST /auth/signup/interests`	Select interests
`POST /auth/signup/profile`	Complete profile (optional)

Auth - Login

Endpoint	Purpose
`POST /auth/login/initiate`	Start login
`POST /auth/login/otp`	Login with OTP
`POST /auth/login/password`	Login with password
`GET /auth/challenge`	Get nonce for device signing

Auth - Device

Endpoint	Purpose
`POST /auth/device/register`	Register device (public key)
`POST /auth/device/verify`	Verify new device OTP
`GET /auth/devices`	List trusted devices
`DELETE /auth/devices/{id}`	Revoke device

Auth - Session

Endpoint	Purpose
`GET /auth/sessions`	List active sessions
`POST /auth/sign-out`	Current device
`POST /auth/sign-out-others`	All except current
`POST /auth/sign-out-all`	Everything

---

12. Database Entities

New Entities

Entity	Purpose
`DeviceKey`	Hardware-bound public keys
`UserSession`	Active sessions
`LoginAttempt`	Risk scoring data
`BlockedUser`	Blocked identifiers/devices
`InterestCategory`	Admin-managed interests
`UserInterest`	User selections
`UsernameChangeHistory`	Track changes

AccountEntity Changes

Field	Change
`password`	Make nullable
`birthDate`	Add
`displayName`	Add
`accountType`	Add (NORMAL, SYSTEM, VERIFIED)
`accountTier`	Add (FULL, RESTRICTED, MINOR)
`authProvider`	Add (PHONE, EMAIL, GOOGLE, APPLE)
`onboardingStep`	Add
`usernameLastChangedAt`	Add
`usernameChangeCount`	Add

---

13. Enums

```
AuthProvider: PHONE, EMAIL, GOOGLE, APPLE
AccountType: NORMAL, SYSTEM, VERIFIED
AccountTier: FULL, RESTRICTED, MINOR
DevicePlatform: IOS, ANDROID, WEB
TrustLevel: HIGH, MEDIUM, LOW
RiskLevel: LOW, MEDIUM, HIGH, CRITICAL
```

---

14. Quick Reference

Onboarding Steps

```
1. Signup (phone/email/OAuth)
2. Verify OTP (if phone/email)
3. Birthdate (age gate)
4. Username
5. Interests (min 3)
6. Profile (optional)
```

Device Verification Matrix

Login Method	Known Device	New Device
OTP	→ Home	→ Home (OTP is verification)
Password	→ Home	→ OTP required → Home
OAuth	→ Home	→ OTP required → Home

Risk Score Quick Reference

```
0-30:   Allow
31-60:  Soft verify
61-85:  Phone OTP
86-100: Block + alert
```

---

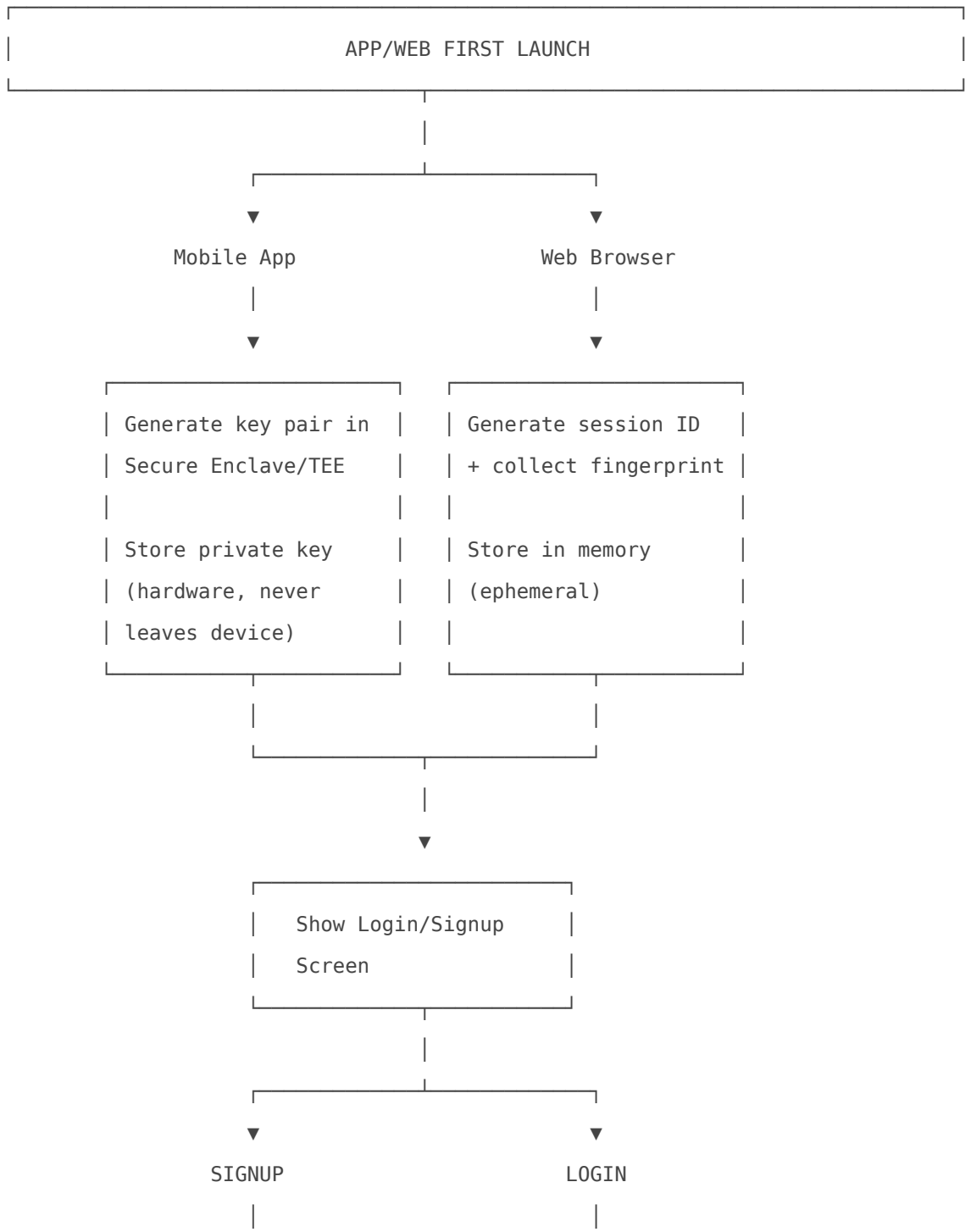
15. Complete Device & Auth Flow (Top to Bottom)

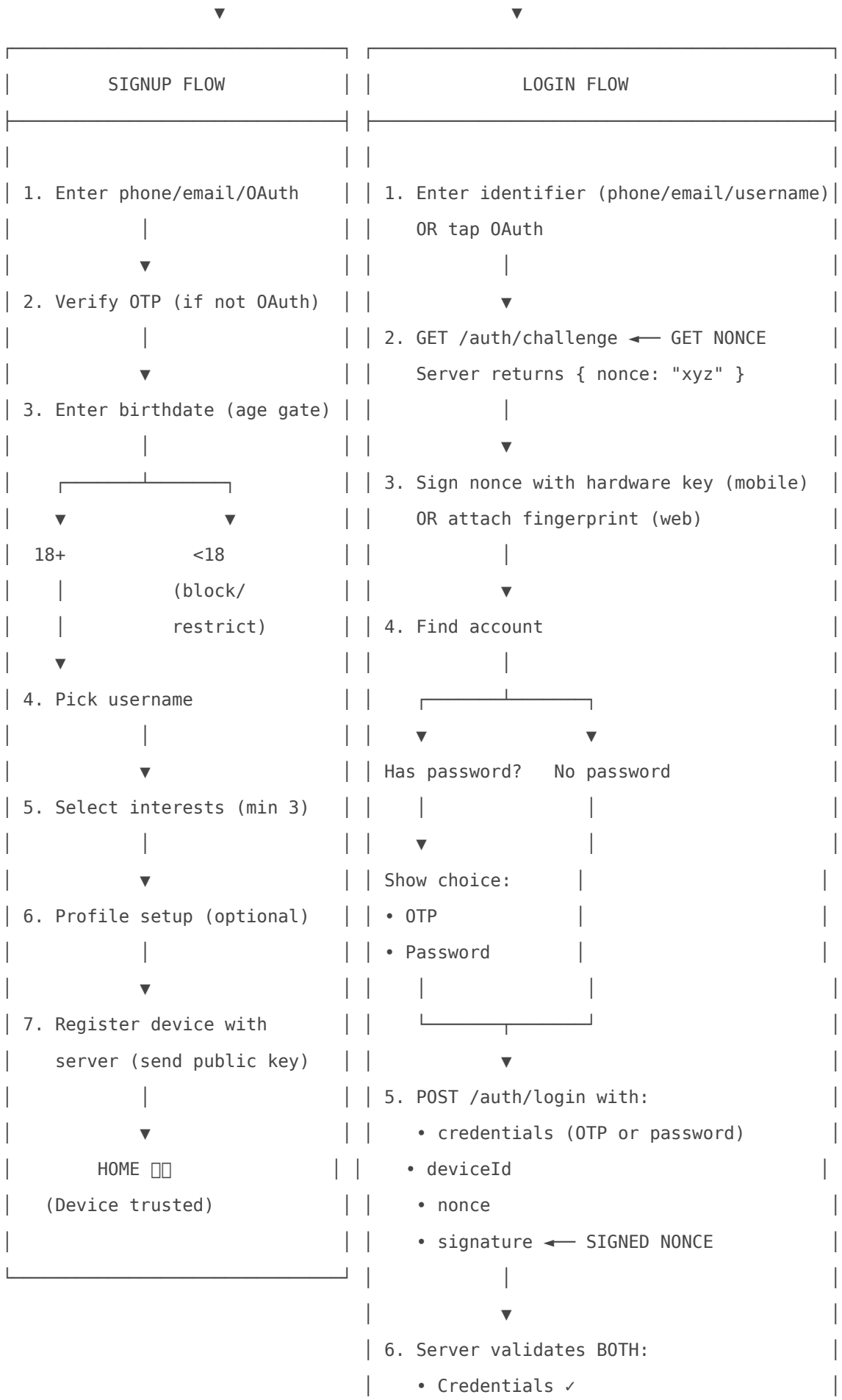
When Does What Happen?

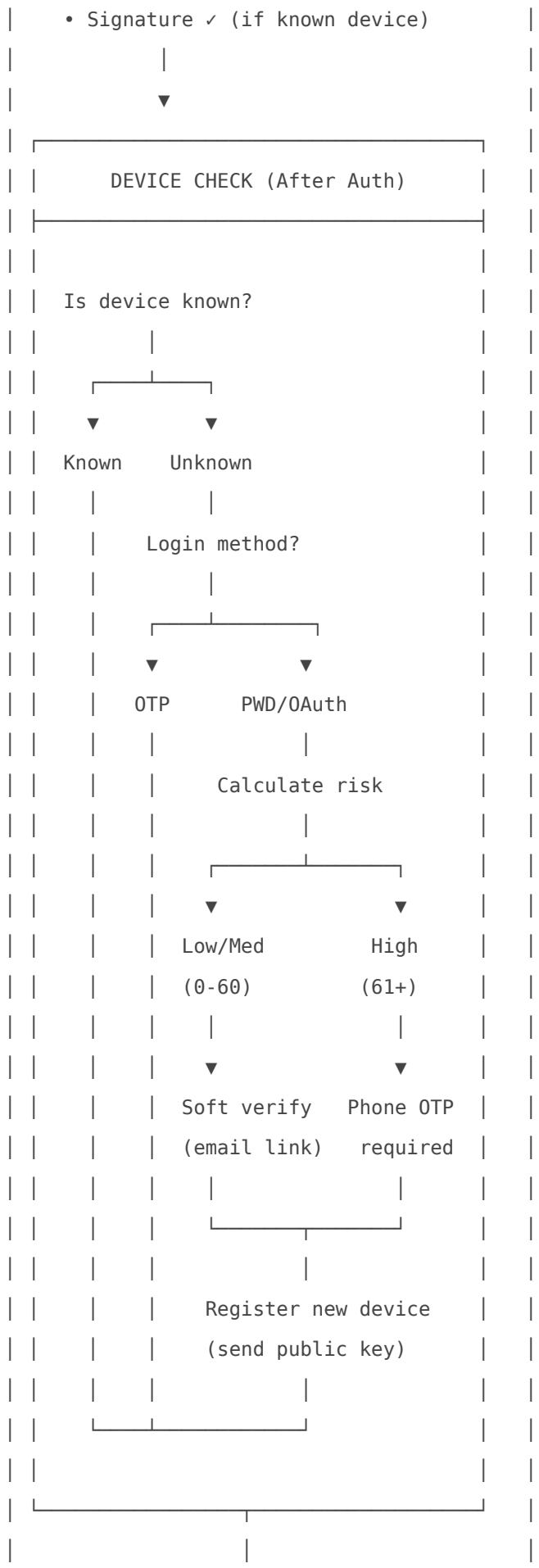
Action	When	Where
Device Registration	First app launch (before any auth)	Mobile only

Action	When	Where
Web Session Init	First visit (before any auth)	Web only
Risk Scoring	After credentials verified, before home	Login only
Device Verification OTP	After risk score (if needed)	Login only (new device + password/OAuth)

Master Flow Chart

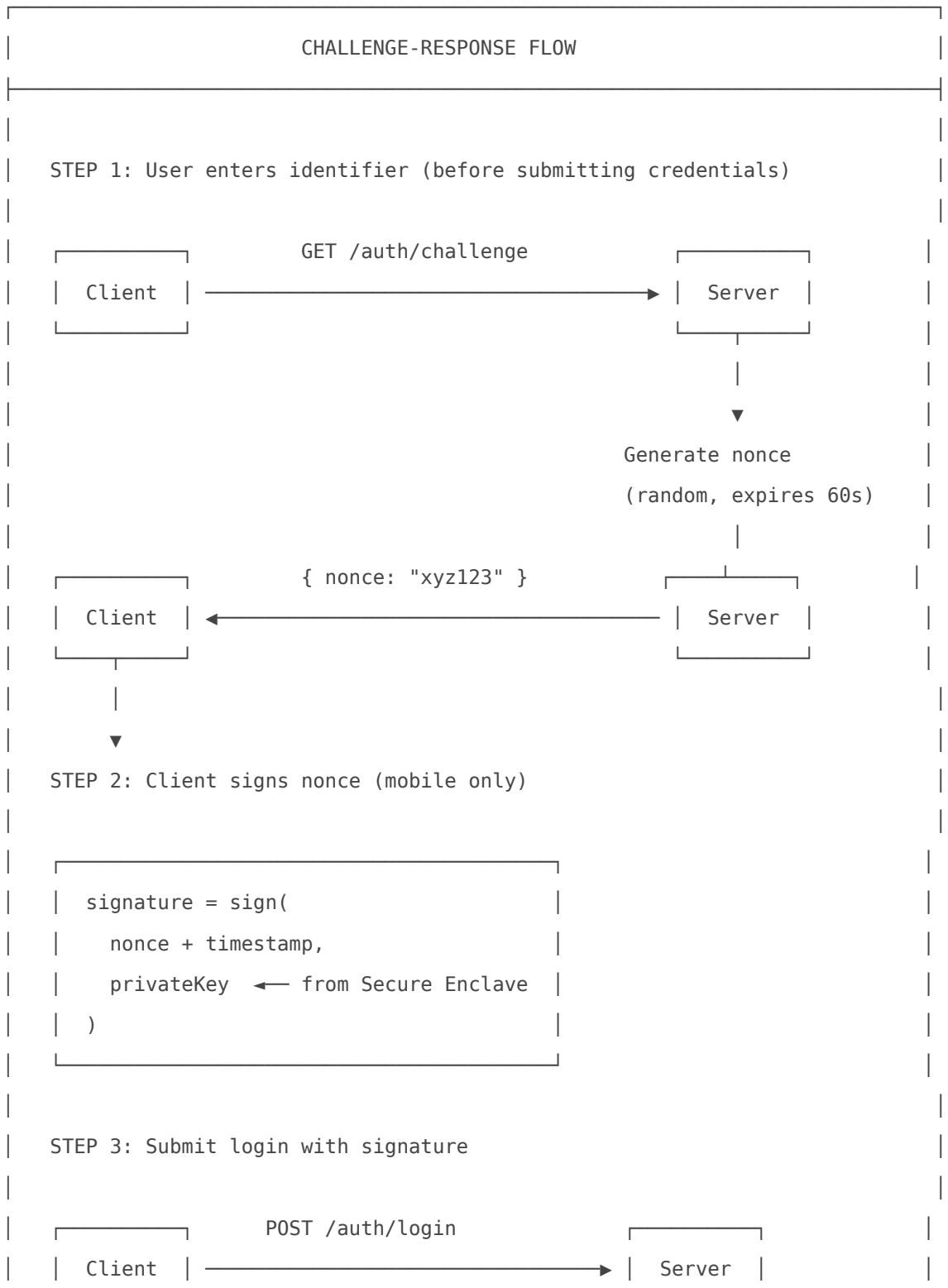


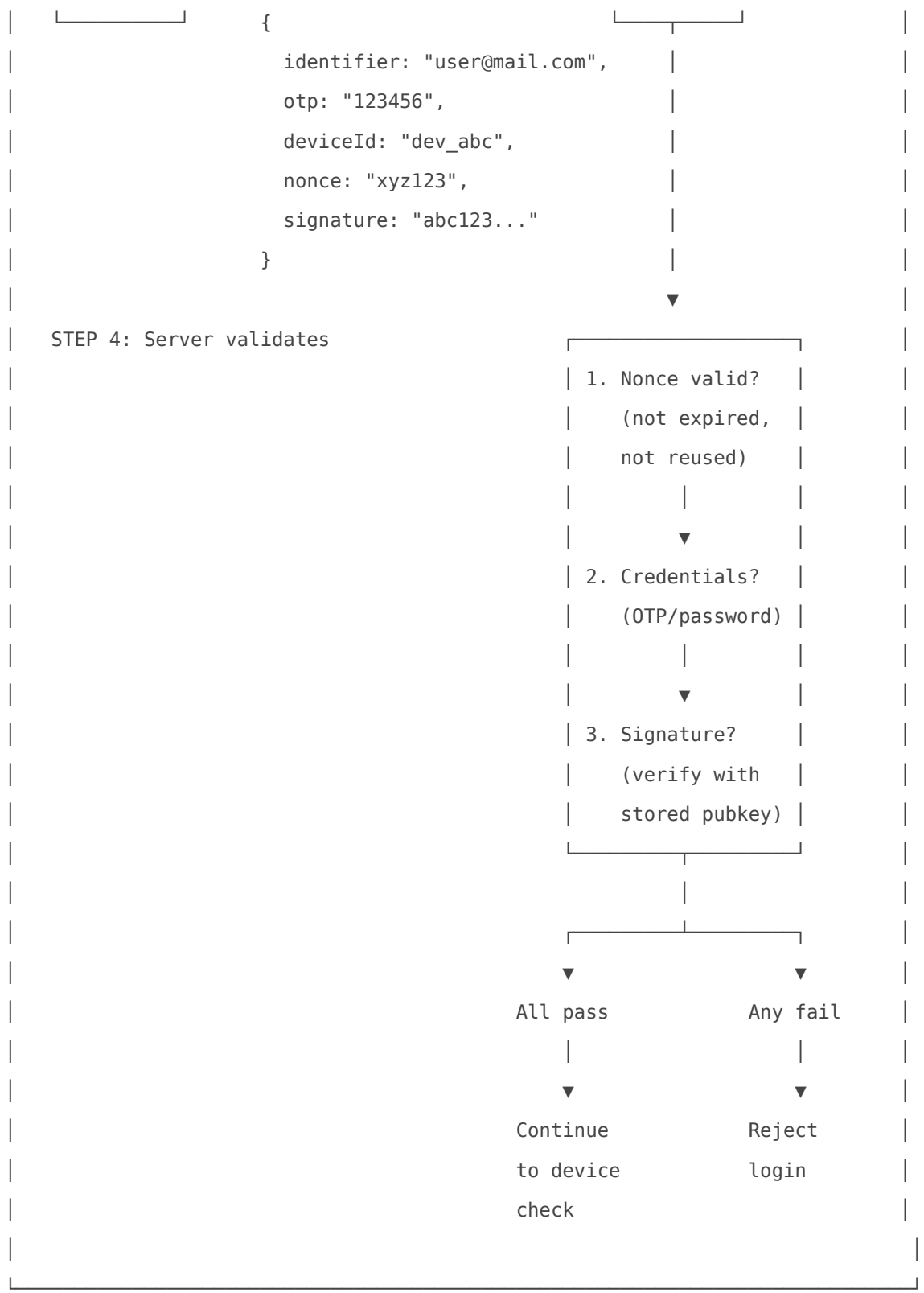

SIGNUP FLOW
1. Enter phone/email/OAuth
2. Verify OTP (if not OAuth)
3. Enter birthdate (age gate)
18+
<18
(block/
restrict)
4. Pick username
5. Select interests (min 3)
6. Profile setup (optional)
7. Register device with
server (send public key)
HOME
(Device trusted)
LOGIN FLOW
1. Enter identifier (phone/email/username)
OR tap OAuth
2. GET /auth/challenge ◄── GET NONCE
Server returns { nonce: "xyz" }
3. Sign nonce with hardware key (mobile)
OR attach fingerprint (web)
4. Find account
Has password?
No password
Show choice:
• OTP
• Password
5. POST /auth/login with:
• credentials (OTP or password)
• deviceId
• nonce
• signature ◄── SIGNED NONCE
6. Server validates BOTH:
• Credentials ✓


• Signature ✓ (if known device)
DEVICE CHECK (After Auth)
Is device known?
Known
Unknown
Login method?
OTP
PWD/OAuth
Calculate risk
Low/Med
(0-60)
High
(61+)
Soft verify
(email link)
Phone OTP
required
Register new device
(send public key)



Challenge-Response: Detailed Flow





When Challenge Happens: Summary

Scenario	Challenge?	Signature Validated?
Signup	❌ No	❌ No (device not registered yet)

Scenario	Challenge?	Signature Validated?
Login - Known device (mobile)	✅ Yes	✅ Yes (must match)
Login - Known device (web)	✅ Yes	✅✅ Fingerprint checked
Login - Unknown device	✅ Yes	❌ No pubkey stored yet

Request/Response Example

1. Get Challenge:

```
GET /auth/challenge

Response:
{
  "nonce": "ch_7f8a9b2c3d4e5f6g",
  "expiresIn": 60
}
```

2. Login with Signature:

```
POST /auth/login

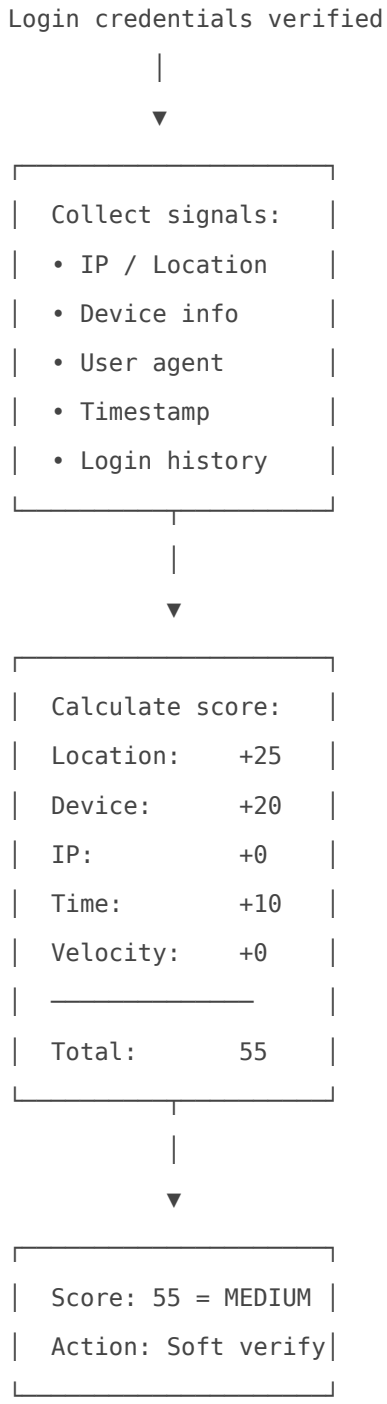
{
  "identifier": "alex@email.com",
  "otp": "123456",
  "deviceId": "dev_iphone14_abc123",
  "nonce": "ch_7f8a9b2c3d4e5f6g",
  "signature": "MEUCIQD2k3n...(base64 signed data)...",
  "timestamp": "2026-01-12T10:30:00Z"
}
```

Signup vs Login: What Happens Where

Step	Signup	Login
Device key generation	✅ Before auth (app launch)	✅ Before auth (app launch)
OTP verification	✅ To verify phone/email	✅ As login method OR device verify
Age gate	✅ After OTP	❌ Not needed
Username	✅ Required	❌ Not needed

Step	Signup	Login
Interests	✅ Required	❌ Not needed
Risk scoring	❌ Not needed (new account)	✅ After credentials verified
Device verification OTP	❌ Not needed (first device)	✅ If new device + high risk
Device registration	✅ End of onboarding	✅ After device verification

Risk Scoring: When & How



16. Logout / Sign Out

Options

Action	What It Does	Requires
Sign out	End current session	Nothing
Sign out other devices	End all except current	OTP or Password
Sign out all devices	End everything	OTP or Password

Flow

```
User taps "Sign out"
        │
        ├── "Sign out" (this device)
        │         │
        │         ▼
        │   Revoke current token
        │         │
        │         ▼
        │   → Login screen
        │
        ├── "Sign out other devices"
        │         │
        │         ▼
        │   Verify (OTP or Password)
        │         │
        │         ▼
        │   Revoke all tokens except current
        │         │
        │         ▼
        │   "Other devices signed out" □
        │
        └── "Sign out all devices"
                  │
                  ▼
          Verify (OTP or Password)
                  │
```

```
                ▼
        Revoke ALL tokens (including current)
                │
                ▼
        → Login screen
```

Session Management Screen

```
┌─────────────────────────────────────┐
│      Active Sessions □□             │
├─────────────────────────────────────┤
│                                     │
│   □□iPhone 14 Pro                   │
│      Dar es Salaam • Active now     │
│      This device              [●]   │
│                                     │
│   □□Chrome on Windows               │
│      Nairobi • 2 hours ago          │
│                       [Sign out]    │
│                                     │
│   □□Samsung Galaxy S23              │
│      Mombasa • Yesterday            │
│                       [Sign out]    │
│                                     │
├─────────────────────────────────────┤
│                                     │
│   [Sign out other devices]          │
│                                     │
│   [Sign out all devices] ⚠□         │
│                                     │
└─────────────────────────────────────┘
```

Sign Out Endpoints

Endpoint	Purpose
`POST /auth/sign-out`	Current device
`POST /auth/sign-out-others`	All except current
`POST /auth/sign-out-all`	Everything

Endpoint	Purpose
`DELETE /auth/sessions/{id}`	Specific session

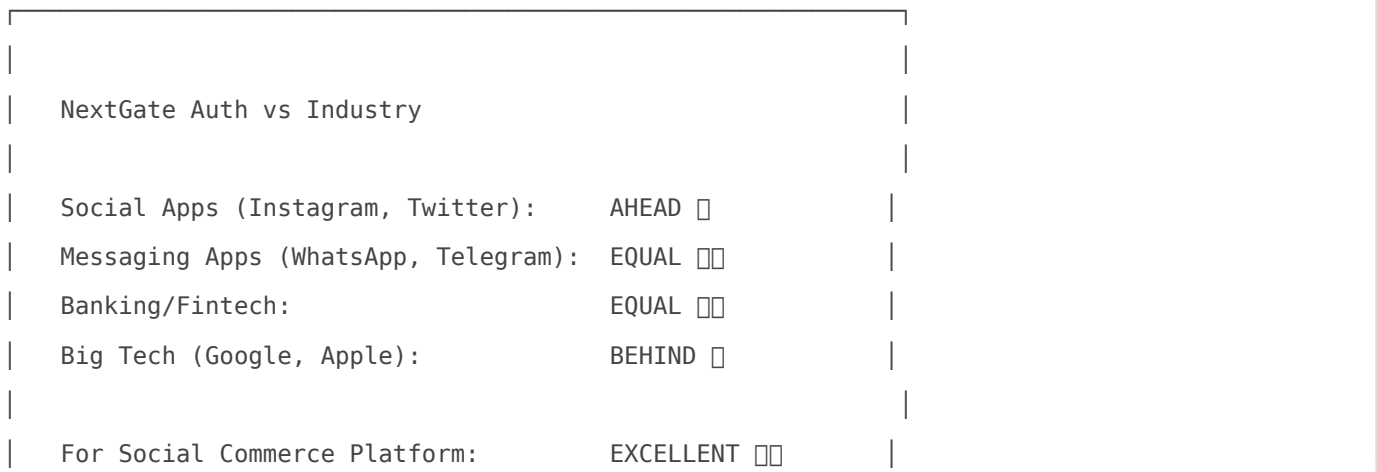
---

18. Industry Comparison

NextGate vs Major Platforms

Feature	NextGate	Instagram	Twitter/X	WhatsApp	Banking Apps
Passwordless default	✅ Yes	❌ No	❌ No	✅ Yes	⚠️ Some
Hardware-bound keys	✅ Yes	❌ No	❌ No	❌ No	✅ Yes
Risk-based auth	✅ Yes	⚠️ Basic	⚠️ Basic	❌ No	✅ Yes
Device trust	✅ Advanced	⚠️ Basic	⚠️ Basic	⚠️ Basic	✅ Advanced
Impossible travel detection	✅ Yes	⚠️ Limited	⚠️ Limited	❌ No	✅ Yes
Session management	✅ Full	✅ Full	✅ Full	⚠️ Limited	✅ Full
Age verification	✅ Tiered	⚠️ Basic	⚠️ Basic	❌ No	✅ Yes
Username change limits	✅ Smart	⚠️ 14 days	⚠️ Limited	✅ N/A	✅ N/A
2FA options	✅ OTP	✅ OTP/App	⚠️ Paid	❌ No	✅ Multiple

Where We Stand



Our Advantages

Over	Advantage
Instagram/Twitter	Hardware-bound device keys, passwordless default
WhatsApp	Multi-identifier login, risk scoring, age gates
Basic apps	Challenge-response auth, impossible travel detection

Future Improvements (v2)

Feature	Impact	Effort
Passkeys/WebAuthn	+0.5 rating	Medium
Backup codes	+0.2 rating	Low
Breach monitoring	+0.2 rating	Low
ML anomaly detection	+0.3 rating	High

Rating: 8.5/10 ?

Verdict: Enterprise-grade auth for a social commerce platform. Better than most social apps, equal to fintech.

Version: 1.0
Status: Ready for implementation

Revision #5
Created 12 January 2026 09:00:17 by Admin Qbit
Updated 3 April 2026 10:40:05 by Admin Qbit