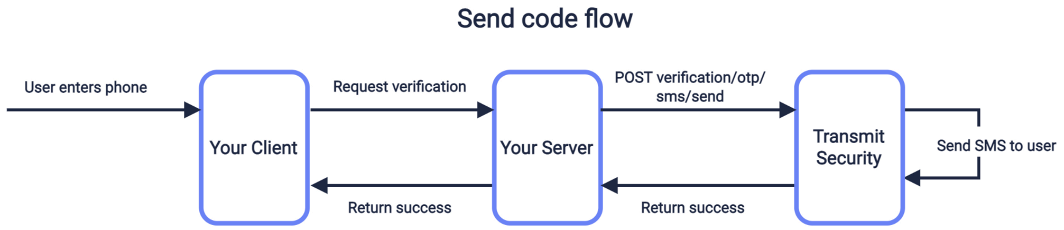
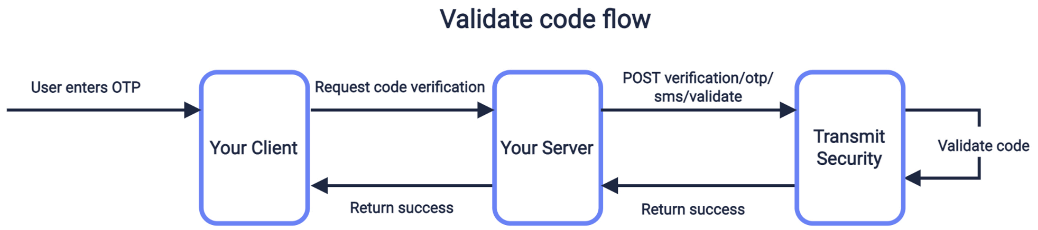
Kiosk Mode:

Kiosk Mode is a special operating mode where a **device is locked to a single app or limited set of apps**, restricting user access to system functions like:

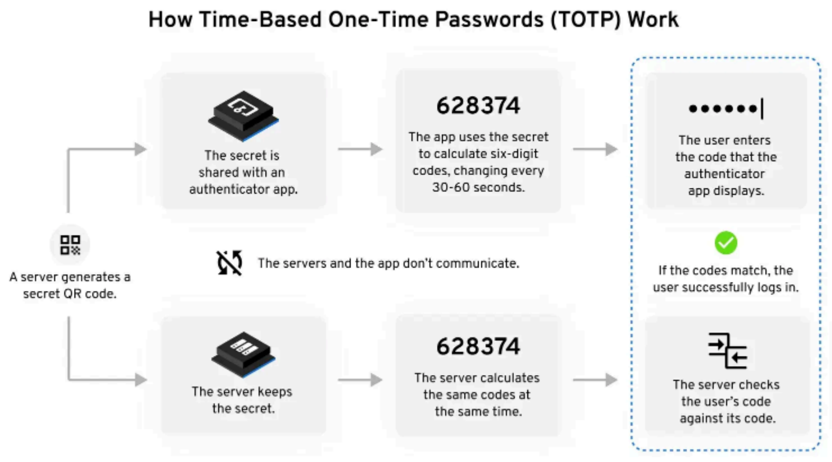
- Home button
- Recent apps
- Notifications
- Status bar
- Navigation gestures
- Settings.

OTP Based authentication:

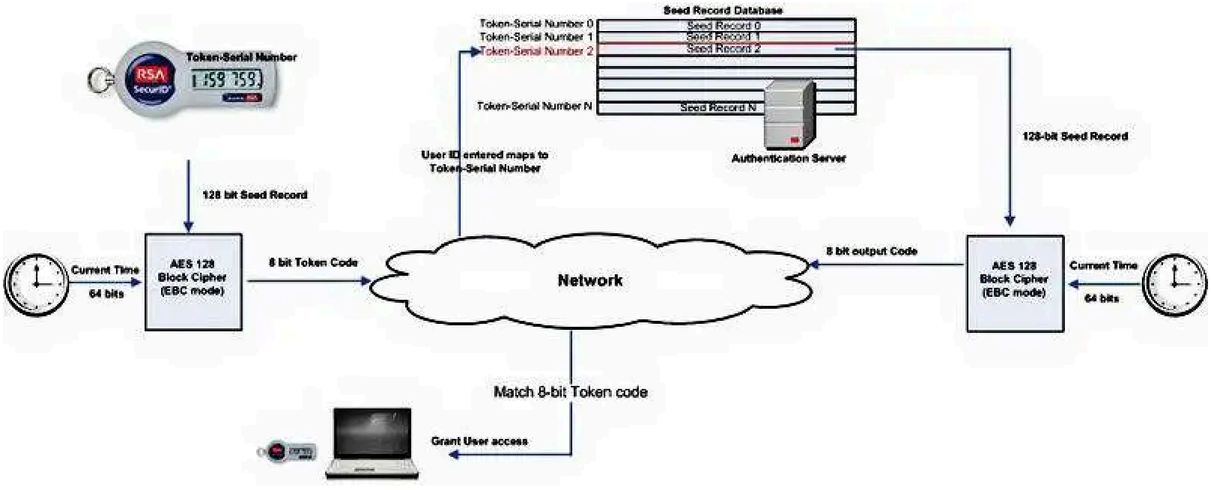




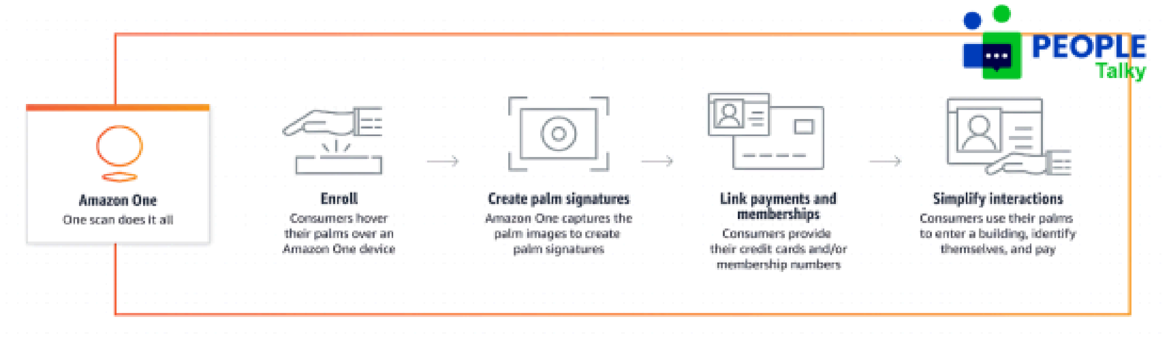
Authenticators:


How Time-Based One-Time Passwords (TOTP) Work
A server generates a secret QR code.
The secret is shared with an authenticator app.
628374
The app uses the secret to calculate six-digit codes, changing every 30-60 seconds.
••••••|
The user enters the code that the authenticator app displays.
The servers and the app don't communicate.
If the codes match, the user successfully logs in.
The server keeps the secret.
628374
The server calculates the same codes at the same time.
The server checks the user's code against its code.

RSA:



PALM Authentication:


PEOPLE
Talky
Amazon One
One scan does it all
Enroll
Consumers hover their palms over an Amazon One device
Create palm signatures
Amazon One captures the palm images to create palm signatures
Link payments and memberships
Consumers provide their credit cards and/or membership numbers
Simplify interactions
Consumers use their palms to enter a building, identify themselves, and pay

+
=
Your hands are uniquely yours
The combination of palm lines, ridges, and subsurface patterns of the palm make it harder for bad actors to steal or mimic.
The Amazon One device is designed to read them
Nothing is stored on the device and images are transmitted with end-to-end encryption to the cloud and stored in a secure zone.
To create your unique palm signature
Users are required to hover their palm over the device each and every time they decide to use it, so there's no risk of incidental identification.

How fingerprint works in our app?

How It Works – Step-by-Step

1. User Enrollment (Initial Setup)

- The user sets up biometric authentication on their phone (OS-level setup).
- The bank app then **requests permission** to use those OS-level biometrics via secure APIs.

2. Integration with Device Biometrics

- The bank app uses **biometric APIs provided by the OS**:
    - **Android**: `BiometricPrompt` or older `FingerprintManager`
    - **iOS**: `LocalAuthentication` framework
- The app doesn't directly access biometric data. Instead:
    - The OS handles authentication.
    - The OS tells the app whether the biometric matches or not (true/false response).

3. Authentication Flow

- User opens the banking app and chooses "Login with Fingerprint/Face."
- The app sends a request to the OS.
- OS shows the biometric prompt (fingerprint/face).
- Biometric match occurs **locally on the device** (never sent to a server).
- If successful, the OS sends a **token or success callback** to the banking app.

4. Secure Session Start

- Once authenticated, the app may:
    - **Decrypt a stored token or session key**
    - **Fetch new authentication tokens from the server** (e.g., OAuth token)
    - Continue into the secure session without asking for password.