# Frequently Asked Question

## Fingerprint attendance device K45 Pro

By : ZKTeco India

### Q.1 What is the K45 Pro?

- A biometric time attendance and access control terminal.
- Features a 2.4-inch TFT screen, fingerprint and card authentication.
- Built-in battery backup ensures operation during power outages.

### Q.2 What are its connectivity options?

- Supports TCP/IP and USB Host for data transfer.
- Some models also offer Wi-Fi connectivity.

### Q.3 What is the user capacity?

- Fingerprint capacity: 800 users
- Card capacity: 800 cards
- Record capacity: 80,000 logs.

### Q.4 What are the key functions?

- Access control: Interfaces for electric locks and exit buttons.
- Time attendance: In/out tracking with work codes and scheduled bells.
- Self-service query, T9 input, and multi-language support.

### Q.5 How do I reset the device?

- You can restore factory settings using the number 7 key on boot.
- This will reset parameters and user data, so use with caution.

### Q.6 What software is compatible?

- Works with ZKTime.Net 3.0 for attendance management.
- Supports USB data import/export and ADMS cloud mode.

### Q.6 What are the operating conditions?

- Temperature: 0°C to 45°C
- Humidity: 20% to 80%
- Power supply: DC 12V 1.5A.

# Q: What Is Biometric Authentication?

- **Biometric authentication is a security method that verifies your identity using unique biological traits. These can include:**

- Fingerprints
- Facial features
- Iris or retina patterns
- Voice
- Vein patterns
- Even behavioral traits like how you type or walk

- **How the Process Works**

**Here's a step by step look at how it typically functions:**

## 1. Enrollment

- Your biometric data is captured using a scanner or sensor (e.g., fingerprint reader, camera).
- The system converts this data into a digital template—a mathematical representation of your trait.

## 2. Storage

- The template is securely stored, either on the device (like a biometric terminal) or in a central database.
- It's encrypted to prevent misuse.

## 3. Authentication

- When you attempt to access a system, your biometric is scanned again.
- A new template is created from this scan.

## 4. Matching

- The new template is compared to the stored one.
- If the match is within an acceptable threshold, access is granted.

- **Why It's Secure (and Where It's Used)**

- Hard to fake: Your fingerprint or iris is much harder to replicate than a password.
- Convenient: No need to remember anything—just be yourself.

- Used in: Smartphones, ATMs, border control, offices, and biometric devices like the ZKTeco K45 Pro.

## Things to Keep in Mind

- False rejections can happen if your finger is wet or your face is obscured.
- Privacy concerns exist around how and where biometric data is stored.
- Biometric data is permanent—you can’t change your fingerprint like a password.