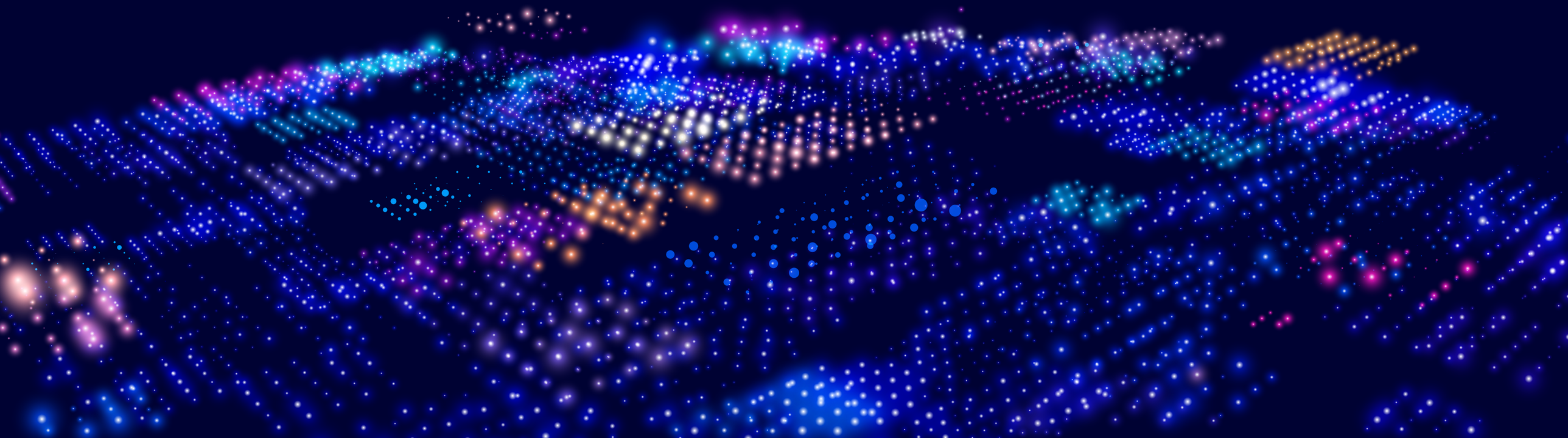
ARMATURA

BioCode - The Ultimate Biometric Access Control Solution



ARMATURA

Biometric-Encrypted QR Code on Smart Phone

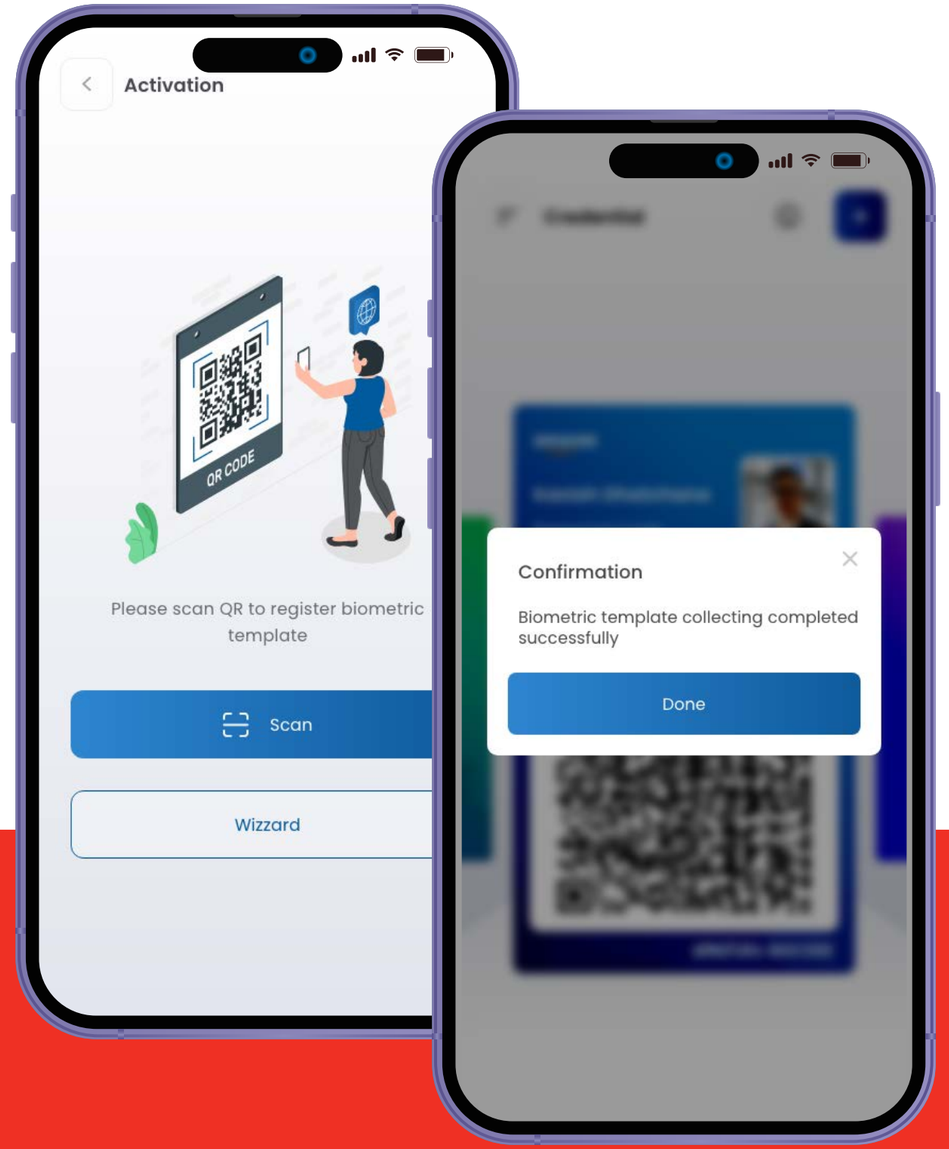
BioCode is a state-of-the-art biometric solution that delivers unparalleled user security and privacy. With BioCode, you get a fully scalable and decentralised system that allows storing all your biometric data and templates on your phone, which can then be converted into a fully encrypted dynamic QR code. This minimize the need for expensive front-end terminals, complicated network infrastructure, and high-speed servers, making BioCode the perfect solution for organisations that demand optimal performance and cost-effectiveness.

ARMATURA

Effortless Biometric Registration with Our Mobile App

Our user-friendly mobile app makes it easy to register your biometrics in just minutes, with a simple selfie for facial recognition or palm photo for touchless palm recognition. Once registered, you can easily display your BioCode on your mobile app and complete biometric recognition.

BioCode leverages advanced biometric technology to deliver lightning-fast recognition speeds of 0.35 seconds for palm recognition and 0.3 seconds for facial recognition. Our solution is equipped with cutting-edge cyber security measures, including the TOTP concept for the dynamic QR code design and AES256 encryption, to ensure your biometric data is always safe and secure.



ENCRYPTION AES 256 ENCRYPTION

100% SECURE TLS CERTIFIED

CERTIFIED CC EAL6+ CERTIFIED

ARMATURA

How it works: Discover our Mobile Biometric Identity Solution

Launch the app and register your palm and face

Launch the BioCode mobile app on your smart device and initiate the biometric identity registration process by scanning both your palm and face on Terminal.

Secure Generation of BioCode

The app can generate a QR code by converting your biometric templates

Presenting BioCode for Authentication

Open the BioCode mobile app, and present the BioCode in front of the terminal.

Biometric Verification

Second Steps, Biometric Verification, it can be either palm or face, depends on which biometric you are using.

Get Access To Secured Area

If both verifications are successful, proceed directly to the assigned area.

BioCode Biometric Algroithum

As a component of the Armatura suite of solutions, the BioCode system employs advanced Armatura Biometric algorithms encompassing touchless palm and facial recognition technologies. Utilising Armatura's cutting-edge biometric capabilities, the system achieves unparalleled recognition speed, distance, and posture adaptability, in addition to robust anti-spoofing measures.

The Armatura research and development team has devoted significant resources to enhance anti-spoofing capabilities by incorporating various techniques. These include liveness detection through infrared technology, palm shape and face detection leveraging deep learning methodologies, and the identification of falsified photos and videos via computer vision techniques. Consequently, Armatura has established itself as one of the industry's most secure biometric solution providers.

Face Recognition Specification（Terminal Side）	
Face Recognition Distance	Dual Camera Liveness Detection: 15.7" - 55.1" (40cm - 140cm) Single Camera Liveness Detection: 15.7" - 78.7" (40cm - 200cm)
Face Recognition Posture Adaptability	Yaw ≤ 30°, Pitch ≤ 30°, Roll ≤ 45°
Face Recognition Accuracy	True Accept Rate (TAR)=99%@, False Accept Rate(FAR)=0.01%
Face Recognition Mode	1:1
Face Recognition Speed	< 100ms (Field Test Result)
Face Recognition Liveness Detection	Yes (Infrared-visible light mode, Infrared Light Mode)
Face Mask Detection	Yes

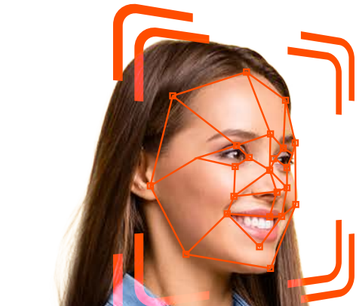
Palm Recognition Specification（Terminal Side）	
Palm Recognition Distance	Liveness Detection On: 7” -15.7” (18cm - 40cm)
Palm Recognition Posture Adaptability	Yaw ≤ 45°, Pitch ≤ 30°, Roll ≤ 90°, Bend ≤ 30°
Palm Recognition Accuracy	True Accept Rate(TAR)=98.7%@, False Accept Rate(FAR)=0.01%
Palm Recognition Mode	1:1
Palm Recognition Speed	< 140ms (Field Test Result)
Palm Recognition Liveness Detection	Yes (Infrared Light Mode)

ARMATURA

Features

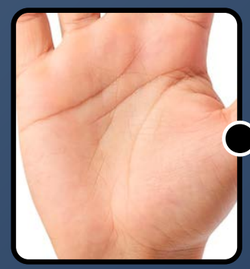
1. Biometric Template Storage on Smart Device Only
2. Secure Biometric Templates Storages
3. Front-end Biometric Verification
4. High-Speed Verification for Large-scale Biometric Application
5. Advanced Security Standards
6. Keep Your Own privacy
7. Scalable Biometric Recognition Solutions
8. Advanced Security with AES256
9. Advanced Biometric Features: Live Detection, Mask Recognition, and More
10. Enhanced Security with Two-FactorAuthentication in BioCode
11. Dynamic QR code for Better Security

ARMATURA



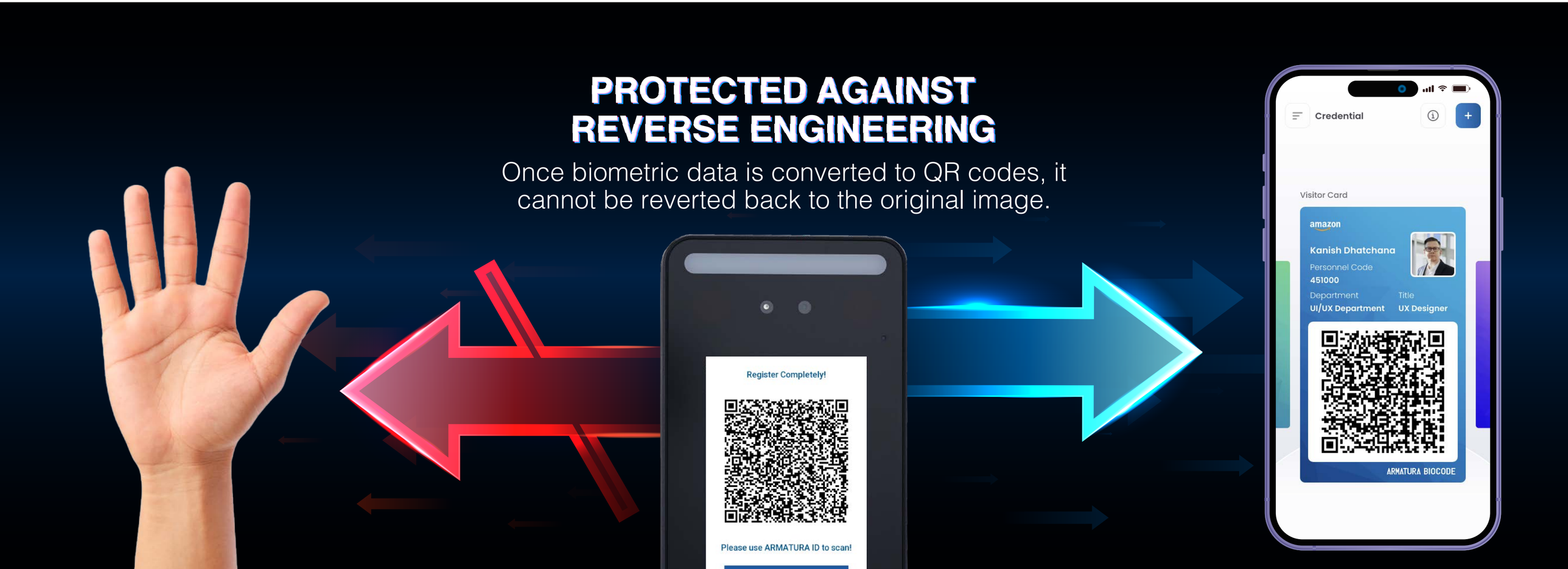
1. Biometric Template Storage on Smart Device Only

At BioCode, we recognise the importance of protecting biometric data and ensuring user privacy. That's why we've developed a system that saves all biometric data and templates solely on the user's smart device. By eliminating the need for storage on software and hardware, we provide users with complete control over their biometric information, the algorithms only using biometric templates for verification instead of biometric images and the ability to delete it at any time in compliance with privacy standards.



2. Secure Biometric Information Storage

We employ various security measures to ensure that biometric information is stored safely and securely. Our biometric templates are irreversible and cannot be reverse-engineered, even by our developers. This ensures that biometric data is stored safely and cannot be accessed by unauthorised parties. Furthermore, when converting biometric templates to dynamic QR codes, we use AES256 encryption standards to protect the data.

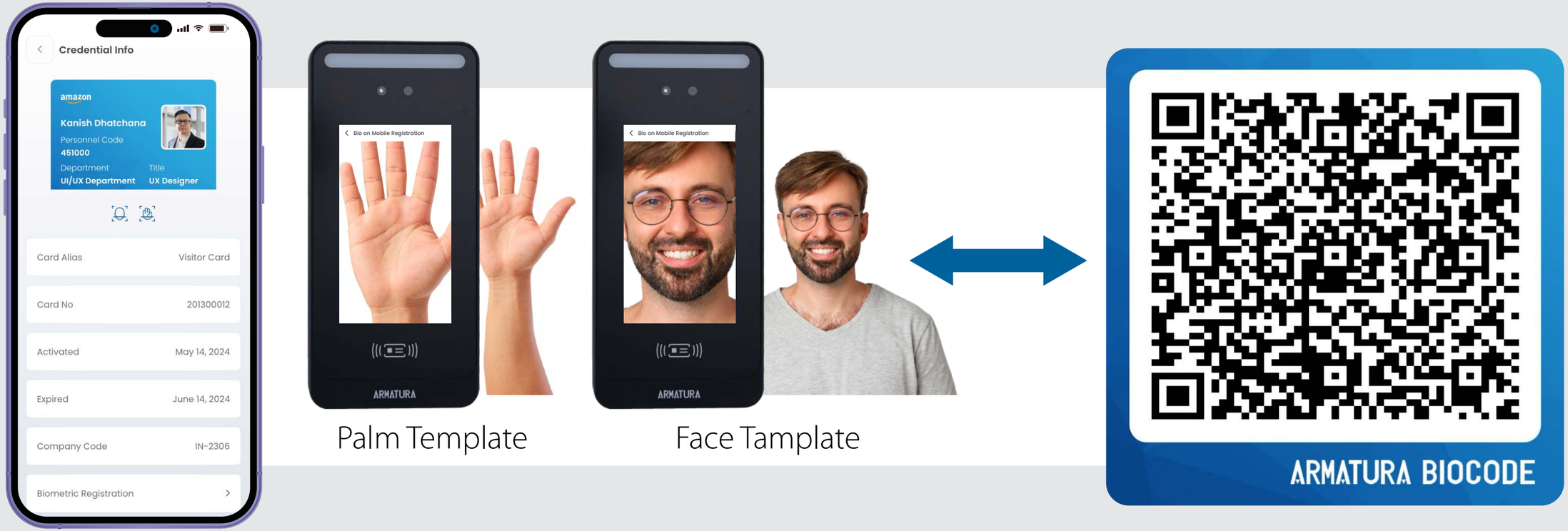


3. Front-end Biometric Verification

BioCode's biometric verification process takes place entirely on the front end, including the QR-code extraction and decryption process. As long as all user profiles are stored on the front end, the system can complete the verification process in completely offline circumstances. This means that BioCode can operate without the need for a network connection, providing an added layer of security and convenience. The only time BioCode requires an online connection is during activation, where the system verifies the user's mobile device.

4. High-Speed Verification for Large-scale Biometric Application

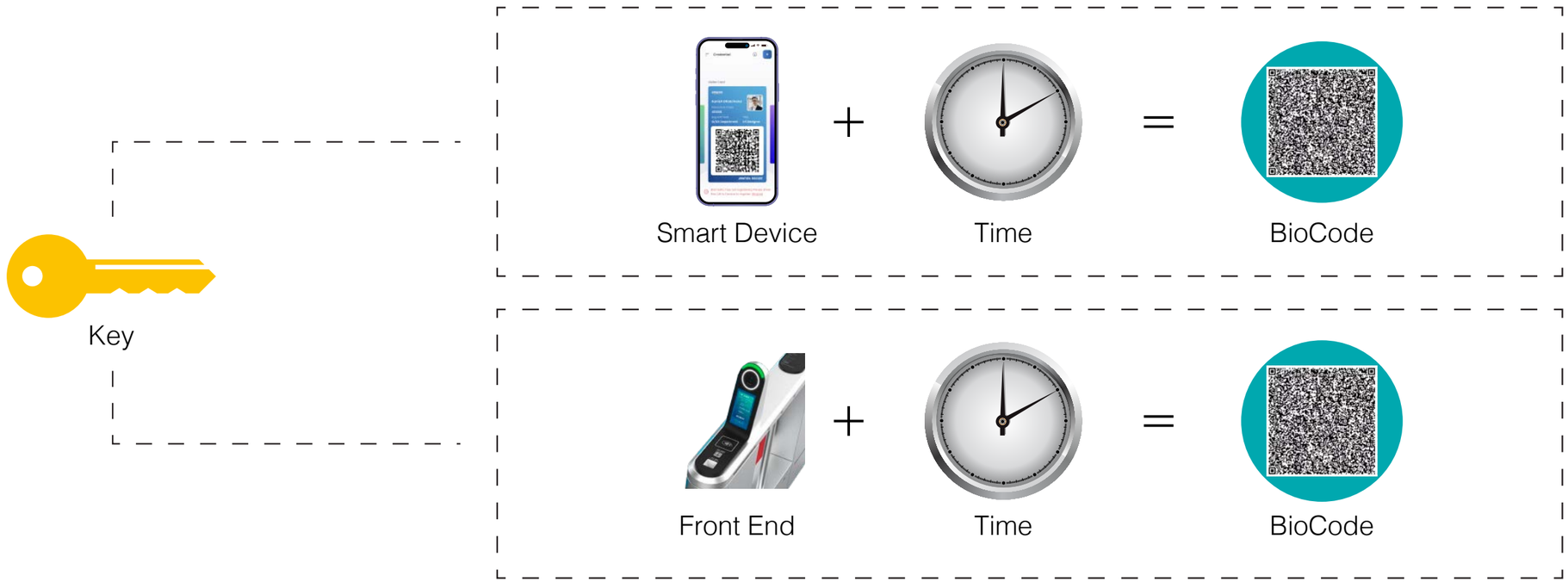
We understand that speed is critical for biometric verification solutions, especially for large-scale deployments. Unlike other large-scale biometric verification methods, BioCode's verification process does not involve backend server communication. This means that the verification process is significantly faster than other solutions, with our lab test results showing that the recognition process can be completed within a second with our advanced biometric technology and user-friendly mobile app.



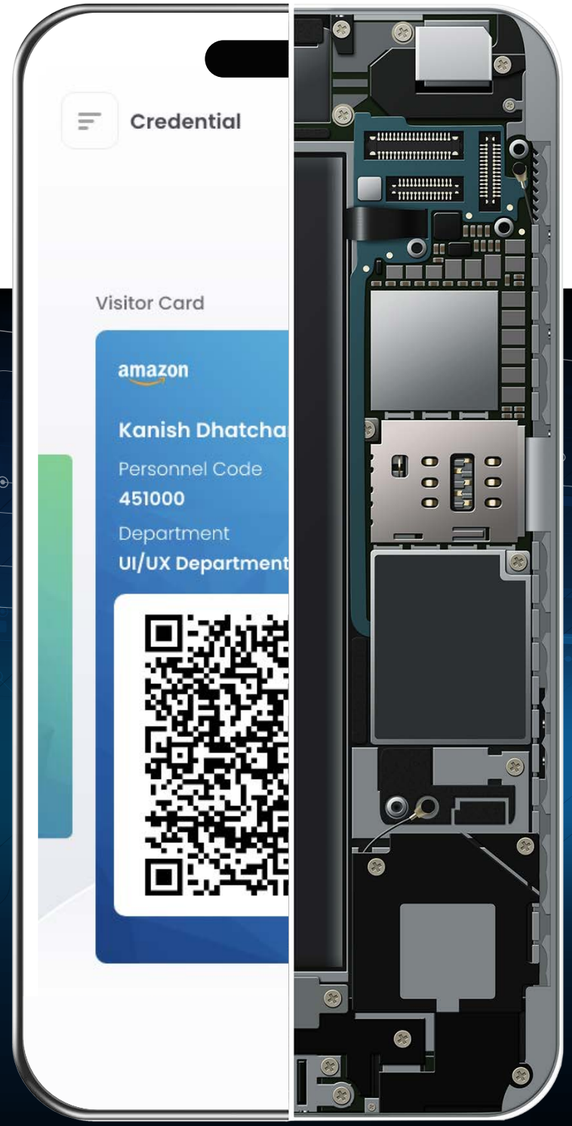
5. Advanced Security Standards

We take cyber security seriously and have incorporated multiple measures to ensure our solution is as secure as possible. To protect against potential attacks, we have implemented the TOTP (Time-based One-Time Password) concept in our dynamic QR code design. This ensures that the QR code will expire in just 3 seconds, making it virtually impossible for attackers to capture a photo of the code and use it maliciously. In addition, we use Armatura's self-developed A.I.-enhanced biometric technology founded on deep learning algorithms, providing superior protection against various biometric spoofing attacks.

TOTP Concept Diagram



ARMATURA



6. Keep Your Own Privacy

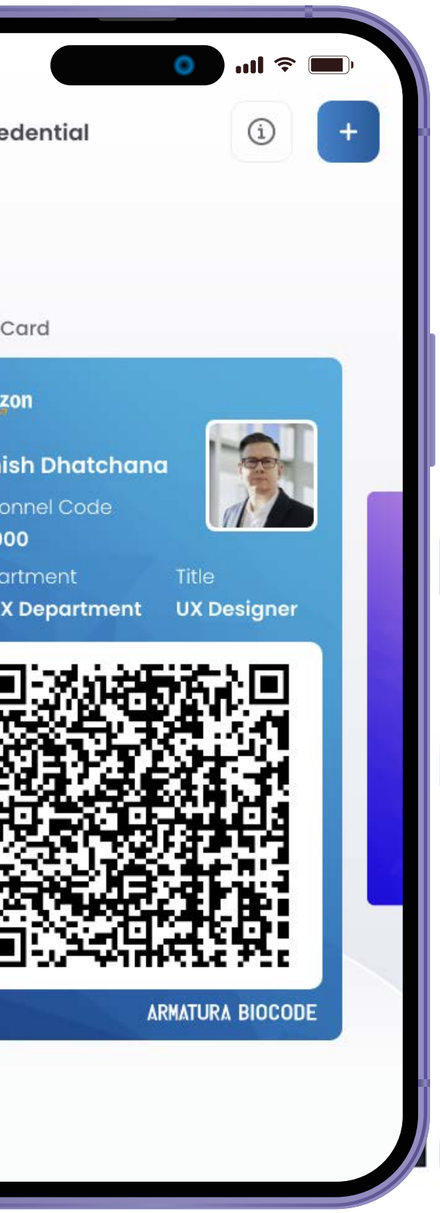
The user's biometric data is solely stored on the user's personal device, ensuring that no external servers or third-party entities have access to this sensitive information. The software and hardware are designed with user privacy as a priority, meaning they do not save, share, or transmit any biometric information beyond the device.

Biometric Data
Solely Stored
on the Smart Device

ARMATURA

7. Scalable Biometrics Recognition Solutions

BioCode is a scalable biometric solution designed to tackle large-scale biometric application scenarios. Unlike other solutions, BioCode can support up to 10 million users without requiring expensive hardware, complicated network architecture, or multiple servers. This makes it an ideal solution for organisations that need to process high volumes of biometric data quickly and efficiently. Our scalable biometric recognition solution is designed to meet the needs of large and small organisations, providing a flexible and cost-effective solution that delivers top-notch performance and security.



8. Advanced Security with AES256

Using AES256, we ensure that all biometric data is encrypted and protected against unauthorised access and potential breaches. This provides an added layer of security and reassurance for organisations that demand the highest levels of security for their biometric data.

9. Advanced Biometric Features: Live Detection, Mask Recognition, and More

BioCode's advanced biometric technology offers a range of enhanced security and convenience features, making it an ideal solution for various applications. In addition to two-factor authentication, BioCode supports live detection and mask recognition.

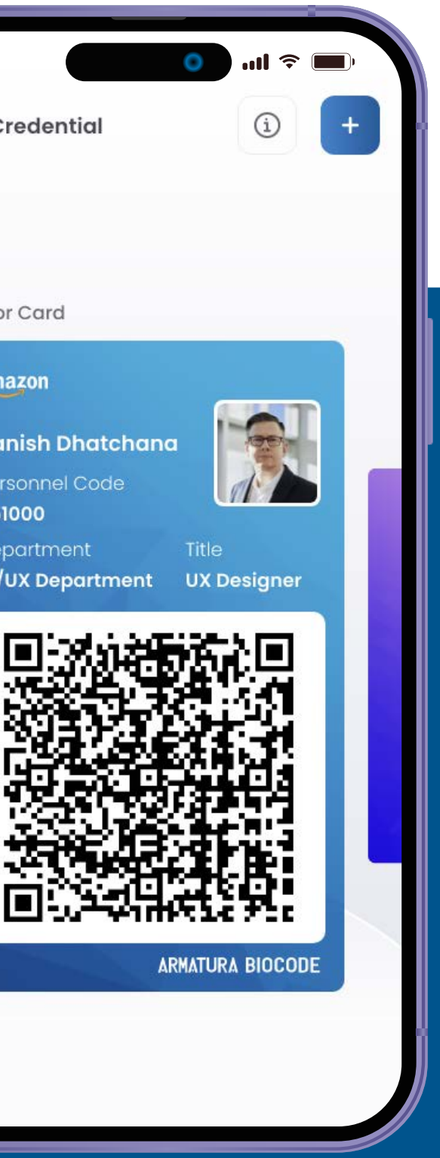
- Mask recognition
  It is another important feature that detects face masks for safe and contactless access control during the pandemic. With this feature, BioCode can recognise a user wearing a mask and adjust the verification process accordingly, providing a safe and convenient solution.

- Live detection
  It is a critical feature that ensures authentic biometric data by preventing spoof attacks. This feature uses advanced algorithms to detect liveness and prevent attackers from using fake biometric data to access secure areas or systems.

ARMATURA

10. Enhanced Security with Two-Factor Authentication in BioCode

BioCode's two-factor authentication combines dynamic QR code and biometric authentication for enhanced security. The QR code serves as the first factor, while biometric authentication provides an additional security factor with users' unique biometric data. This combination ensures highly secure and reliable biometric verification processes.



First Authentication

Dynamic QR Code

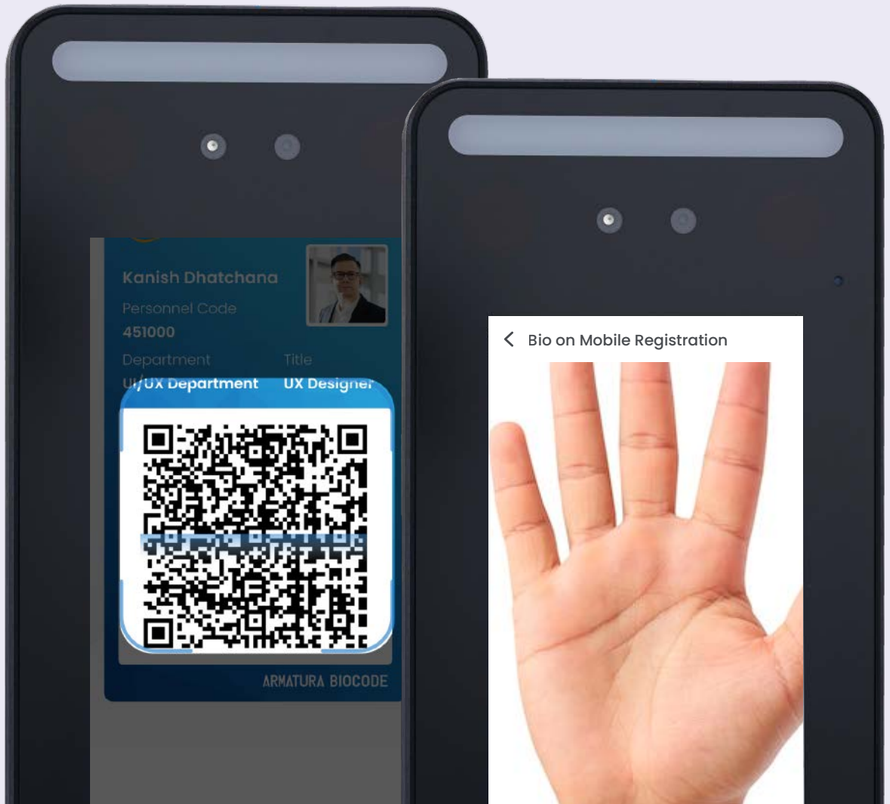
Second Authentication

Palm Recognition

Facial Recognition

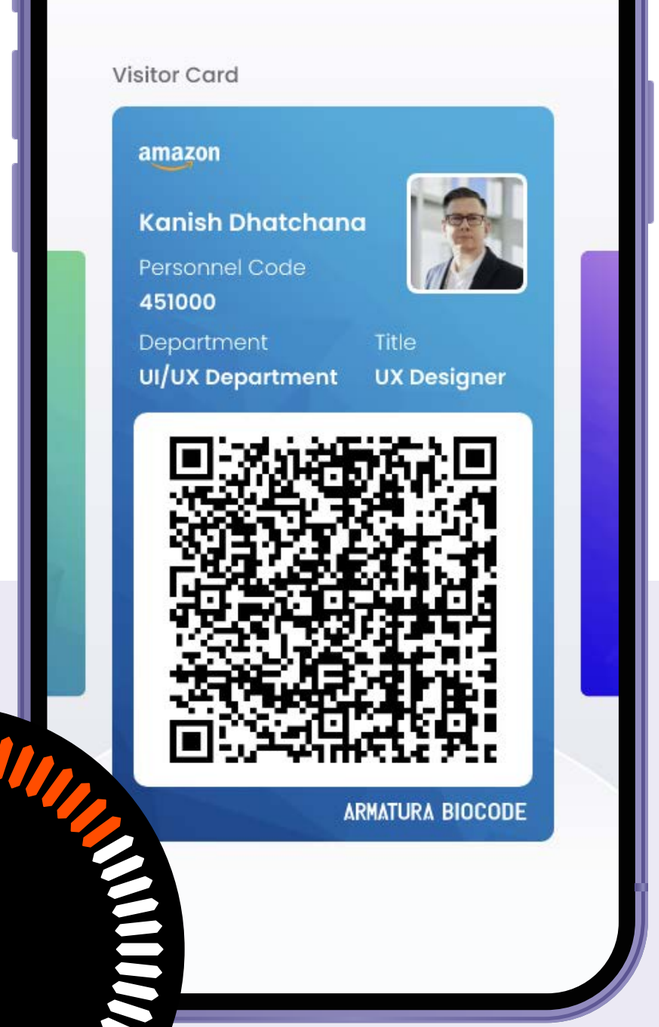
11. Dynamic QR Code for Better Security

To address concerns about potential attacks by copying QR codes, we have implemented a dynamic QR code feature in our mobile app. With this feature, the images of QR codes in the mobile app are set to dynamic, meaning that the QR code images are automatically changed every 2-3 seconds. To ensure the security of the dynamic QR code feature, we use TOTP technology and AES256 protocols during the generation process. This provides an added layer of security and makes it virtually impossible for attackers to copy or use the QR code maliciously.



Dynamic QR Code

Automatic Regenerating New QR-code every 2-3 seconds.



ARMATURA

Competitive Advantages of BioCode Solutions

	Traditional Solution	BioCode Solutions
Cost Effectiveness	Low	High
Hardwares Requirements	High	Low
Server Requirements	High	Low
Privacy Level	Low	High
Security Level	Low	High
Ticket Scalping Prevention	N/A	High
Mobile Tickets	N/A	Yes
Ticketing System Integration	N/A	Yes
Mobile Payment	N/A	Yes

Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.us
Copyright © 2025 Armatura LLC @ ARMATURA, the ARMATURA logo, are trademarks of Armatura