ARMATURA

Biometrics Whitepaper

Secure Multimodal Biometrics for Modern Access Control

Date: April, 2026
Doc Version: 1.0

1. Executive Summary

In an increasingly connected and security-sensitive world, organizations are under growing pressure to protect physical spaces, digital identities, operational assets, and personal data with stronger, more intelligent, and more user-friendly authentication techn ologies. Traditional access credentials such as PIN codes, passwords, RFID cards, and mechanical keys remain widely deployed, but they also introduce structural security limitations. They may be shared, lost, stolen, duplicated, forgotten, or used by unauthorized individuals without a reliable method of confirming the true identity of the person requesting access.

Biometric authentication addresses this challenge by binding access decisions to the unique biological and behavioral characteristics of the individual. Instead of verifying only what a user possesses or remembers, biometric systems verify who the user is. This makes biometrics a powerful foundation for high-assurance access control, identity verification, workforce authentication, visitor management, and secure facility operations.

Armatura's biometric technology is designed to deliver a secure, contactless, privacy-conscious, and scalable authentication experience for modern access control environments. The Armatura biometric architecture combines advanced deep learning, multimodal sensing, liveness detection, feature extraction, irreversible biometric templates, encrypted storage, and intelligent matching to provide reliable identity authentication across a wide range of physical security scenarios.
The core objective of Armatura biometrics is not only to recognize users accurately, but also to establish trust throughout the complete authentication lifecycle. This lifecycle includes biometric acquisition, image quality assessment, anti-spoofing analysis, feature extraction, template generation, template protection, identity comparison, and final access decision. Each stage is designed to strengthen both security and usability.

Armatura's biometric portfolio is built around two primary modalities: deep learning-based face recognition and bi-modal palm authentication. Face recognition provides fast, intuitive, and contactless identity verification by analyzing distinctive facial features and converting them into mathematical representations. Armatura's face recognition pipeline includes face detection, anti-spoofing, face alignment, feature extraction, face embedding, and matching against stored templates. The uploaded technical material describes this inference pipeline as a sequence in which the system detects a face, performs anti-spoofing, aligns the face, extracts high-dimensional facial features, and compares them with stored templates to generate a recognition result.

Bi-modal palm authentication provides an additional high-security contactless option by combining visible-light palm shape recognition with infrared palm vein recognition. Visible-light palm authentication analyzes external palm characteristics such as palm shape, texture, curvature, and finger positions, while infrared palm vein authentication captures internal vein patterns beneath the skin surface. Armatura's own palm authentication material explains that the combination of these two modalities is intended to enhance accuracy and stability while preserving contactless operation.

This multimodal approach provides significant advantages for enterprise security. Face recognition offers speed and convenience in everyday access control scenarios. Palm authentication strengthens authentication assurance through the use of internal palm vein characteristics, which are difficult to observe or replicate. Together, these modalities allow organizations to deploy biometric access control in a way that can be adapted to different risk levels, installation environments, user populations, and operational policies.

Security against spoofing attacks is a central design consideration. Biometric systems are exposed to presentation attacks, where an attacker attempts to deceive the system using printed photos, videos, masks, prosthetics, fake palms, gloves, screen replays, or other artificial media. Armatura's face anti-spoofing material describes the use of visible-light and near-infrared inputs, liveness scoring, face quality assessment, and feature-level analysis to help distinguish genuine users from spoofing attempts. Similarly, Armatura's palm authentication material describes palm liveness detection based on factors such as reflection patterns, material texture, light distribution, surface structure, and the unique properties of palm vein patterns under infrared imaging.

Privacy and biometric data protection are equally important. Armatura's biometric system is designed around the principle that biometric images should not be stored as reusable raw images after the required features have been extracted. According to the uploaded Armatura irreversibility document, the system collects biometric data such as facial and palm images, preprocesses the data, extracts only the necessary biometric features for authentication, and does not store the original images in order to reduce the risk associated with image theft. The same material states that only a portion of the original biometric information required for authentication is retained, while unnecessary information is discarded, making the resulting templates non-interpretable and not usable for reconstructing the complete biometric image.

Armatura further protects biometric templates and other sensitive user information through encryption. The uploaded template protection material states that Armatura applies AES-256 encryption to biometric templates and extends encryption to other sensitive user information such as usernames, user IDs, and user photos during storage and transmission. This approach supports a privacy-by-design security model in which biometric authentication is not treated as a single algorithmic function, but as a protected end-to-end system.

The purpose of this whitepaper is to provide clients, consultants, system integrators, security architects, and enterprise decision-makers with a structured technical understanding of Armatura biometric technology. It explains the role of biometrics in modern access control, introduces Armatura's multimodal recognition architecture, describes the technical foundation of face and palm authentication, outlines anti-spoofing and liveness detection principles, and establishes the importance of template irreversibility and secure biometric data protection.

This whitepaper also provides a foundation for evaluating biometric systems not only by recognition speed or convenience, but by the complete set of security characteristics that matter in real-world deployments: accuracy, resistance to spoofing, template protection, user privacy, system scalability, operational reliability, deployment flexibility, and responsible data governance.

In summary, Armatura biometrics are designed to support the next generation of secure access control: contactless, intelligent, privacy-aware, scalable, and resistant to modern identity threats. By integrating deep learning-based face recognition, bi-modal palm authentication, liveness detection, irreversible biometric templates, and encrypted data protection, Armatura enables organizations to move beyond credential-based access toward a more trusted identity-driven security architecture.

2. The Evolution of Secure Access Control

Access control has traditionally been based on three categories of authentication: something a person knows, something a person has, and something a person is. Early physical access control systems relied heavily on keys, PIN codes, passwords, and ID cards. These methods remain useful in many environments, but they also create operational and security weaknesses when used as the only method of authentication.

A PIN code can be shared. A password can be guessed or phished. A card can be lost, borrowed, cloned, or stolen. A mechanical key can be duplicated. Even when these credentials are assigned to a specific user, they cannot always prove that the authorized user is physically present at the point of access. In other words, traditional credentials authenticate the credential, not necessarily the person.

This distinction has become increasingly important as organizations face more complex security requirements. Modern enterprises must protect offices, data centers, laboratories, airports, campuses, healthcare facilities, manufacturing plants, financial institutions, critical infrastructure, and other sensitive locations. Many of these environments require a higher level of assurance than a standalone card or PIN can provide. They need to know not only that a valid credential has been presented, but that the credential is being used by the legitimate person.

Biometric access control evolved to address this gap. By using measurable human characteristics, biometric systems can directly associate an authentication event with a person's physical identity. Face, palm, fingerprint, iris, and other biometric modalities can help organizations reduce credential sharing, improve auditability, simplify user experience, and strengthen access control policies.

However, biometric technology itself has also evolved. Early biometric systems were often limited by environmental conditions, slower processing speed, user inconvenience, and inconsistent performance across large populations. Some systems required physical contact, fixed positioning, or controlled lighting conditions. Others depended on handcrafted features that were less robust against real-world variation. As a result, biometric adoption historically required careful balancing between security, convenience, and reliability.

The rise of deep learning and advanced sensor technology has significantly changed this landscape. Deep neural networks can learn complex, discriminative features from large datasets and can improve recognition performance under challenging conditions. Armatura's deep learning face recognition material describes deep learning as a technology that automatically learns hierarchical representations from data, extracting increasingly complex features through multiple neural network layers. For face recognition, this allows the system to learn facial representations that can distinguish between individuals even when real-world variation exists.

Modern biometric systems also increasingly use multimodal sensing. Instead of relying on a single image type or a single biometric characteristic, multimodal systems combine multiple sources of identity evidence. This makes authentication more robust because different modalities compensate for each other's limitations. Armatura's bi-modal palm authentication is an example of this design principle. Visible-light palm recognition provides useful external palm information, while infrared palm vein recognition captures internal vein characteristics beneath the skin surface.

The evolution of access control is therefore moving in three major directions.

First, access control is moving from credential-based verification to identity-based verification. A secure facility must know who is entering, not only which card or code was used. Biometrics directly support this transition by linking access events to physical identity.

Second, access control is moving from isolated authentication devices to intelligent security ecosystems. Modern systems need to integrate terminals, controllers, management software, mobile credentials, cloud platforms, visitor systems, APIs, and enterprise directories. Biometric authentication must therefore operate as part of a complete access control architecture rather than as an isolated recognition function.

Third, access control is moving from basic recognition to trusted authentication. Recognition accuracy alone is no longer sufficient. A biometric system must also determine whether the biometric sample is genuine, whether the image quality is acceptable, whether the template is protected, whether user privacy is preserved, and whether the system can operate reliably at scale.

This is where liveness detection and anti-spoofing become essential. Presentation attacks are among the most important risks in biometric security. Attackers may attempt to use printed photos, videos, 3D masks, prosthetic faces, fake hands, gloves, palm images on mobile screens, or other artificial objects to impersonate an enrolled user. Armatura's facial anti-spoofing material identifies presentation attacks such as prints, videos, 3D masks, and

makeup, and describes face anti-spoofing as a critical technology for strengthening face recognition systems. For palm authentication, Armatura's liveness detection approach is designed to analyze both visible and infrared information. The system evaluates characteristics such as reflection, material texture, light distribution, surface structure, and the unique liveness properties associated with palm vein patterns. This allows the system to help differentiate genuine palms from printed images, screen displays, gloves, fake hands, and other spoofing media.

Another major change in the evolution of access control is the increasing importance of privacy and data governance. Biometric data is sensitive because it relates directly to the individual. Therefore, a modern biometric access control system must be designed to minimize data exposure, protect templates, avoid unnecessary storage of raw images, and support responsible data management.

Armatura's template protection architecture addresses this concern by focusing on feature extraction and template irreversibility. The system extracts the biometric features needed for authentication and discards unnecessary biometric information. The uploaded Armatura document states that complete biometric images are not stored after feature extraction and that the stored templates cannot be interpreted or reversed to reconstruct the original biometric images. This design principle is fundamental to building client trust in biometric deployments.

The future of secure access control will be defined by systems that combine assurance, convenience, intelligence, and privacy. Organizations no longer want security technologies that create friction, slow down entry, or expose unnecessary personal data. They need authentication methods that are fast enough for daily operations, secure enough for high-risk environments, flexible enough for different deployment scenarios, and responsible enough for modern privacy expectations.

Armatura's biometric technology is positioned within this new generation of access control. It combines contactless face recognition, contactless bi-modal palm authentication, liveness detection, irreversible templates, encrypted biometric data protection, and scalable recognition architecture. This allows organizations to strengthen security without sacrificing user experience.

In this new model, access control is no longer simply a door-opening mechanism. It becomes an identity assurance layer for the enterprise. Every authentication event becomes a trusted decision supported by biometric evidence, anti-spoofing intelligence, protected templates, and centralized policy enforcement. This is the direction in which modern physical security is moving, and it is the technical foundation upon which Armatura's biometric architecture is built.

3. Armatura Multimodal Biometric Technology Overview

Armatura's biometric technology is built on a multimodal authentication strategy that combines advanced recognition algorithms, intelligent sensing, liveness detection, privacy protection, and secure template management. The purpose of this architecture is to support reliable identity authentication across modern access control environments, from corporate facilities and smart buildings to high-security sites and large-scale enterprise deployments.

A multimodal biometric system uses more than one biometric modality or more than one type of sensing information to strengthen identity verification. Compared with single-modality authentication, multimodal biometrics can improve resilience, reduce dependence on a single biometric trait, and provide greater flexibility for different user groups and environmental conditions.

Armatura's current biometric technology can be understood through three main pillars:

1. Deep learning-based face recognition
2. Bi-modal palm authentication
3. Biometric template protection and secure data processing

Together, these pillars create a biometric authentication platform that is fast, contactless, secure, and suitable for integration into enterprise access control systems.

3.1 Deep Learning-Based Face Recognition

Face recognition is one of the most intuitive biometric modalities for access control. It enables users to authenticate naturally and contactlessly, without presenting a card, touching a sensor, or entering a PIN. This makes it highly suitable for office entrances, turnstiles, lobby access, restricted zones, visitor workflows, and high-throughput environments.

Armatura's face recognition technology is based on deep learning. In general, deep learning models learn layered representations from data, allowing the system to extract meaningful facial features automatically instead of relying only on manually designed feature rules. Armatura's face recognition material explains that deep learning-based face recognition uses deep neural networks to identify and verify individuals based on facial features, using labeled face images to learn discriminative features that distinguish different individuals.

The face recognition process includes several major stages.

First, the system detects and locates the face within the image or video frame. Face detection determines whether a face is present and where it is positioned.

Second, the system performs anti-spoofing and quality-related checks. This helps determine whether the detected face is likely to be a live person rather than a spoofing medium such as a printed image, video, mask, or other presentation attack.

Third, the system aligns the face. Face alignment normalizes the detected face into a standard coordinate structure so that variations in pose, scale, and orientation can be reduced before feature extraction.

Fourth, the system extracts facial features using deep neural networks. These features are converted into a mathematical representation, commonly referred to as a face embedding.

Finally, the face embedding is compared with stored templates to verify or identify the individual. In a 1:1 verification scenario, the system compares the user against a claimed identity. In a 1:N identification scenario, the system searches across a database of enrolled users to determine the closest matching identity.

The uploaded Armatura face recognition material describes this inference pipeline as a sequence consisting of face detection, face anti-spoofing, face alignment, face feature extraction, and face embedding/matching. This structure reflects a complete recognition architecture rather than a simple image comparison mechanism.

Armatura's face recognition technology also incorporates advanced training concepts such as distortion-invariant recognition and masked-face recognition. These are important because access control environments are rarely perfect. Camera angles, lens distortion, lighting variation, user movement, partial occlusion, and face coverings can all affect recognition quality. Armatura's uploaded material describes distortion-invariant face recognition as a method intended to reduce the effect of radial lens distortion, and

masked-face recognition as a training approach that improves the model's ability to recognize faces under occlusion.

3.2 Facial Liveness Detection and Anti-Spoofing

Face recognition must be protected against presentation attacks. A high-accuracy recognition algorithm is not sufficient if the system can be deceived by a non-live representation of an authorized user. For this reason, liveness detection is an essential part of Armatura's face recognition architecture.

Armatura's face anti-spoofing approach uses multimodal sensing and deep learning-based analysis to help determine whether the face presented to the system belongs to a genuine live person. The uploaded material describes the use of visible-light and near-infrared inputs, feature extraction from both modalities, liveness scoring, and fusion-based decision-making.

During the anti-spoofing process, the system analyzes characteristics that may indicate whether the input is live or artificial. These may include texture, reflection, depth-related information, light distribution, material differences, and other visual or spectral cues. Armatura's material identifies common presentation attack types such as printed photos, videos, 3D masks, and makeup.

The purpose of this anti-spoofing layer is to ensure that recognition is performed only after the system has established sufficient confidence that the biometric sample is genuine. In an access control environment, this is critical because the system must defend not only against accidental recognition errors, but also against intentional impersonation attempts.

3.3 Bi-Modal Palm Authentication

Palm authentication is an increasingly important biometric modality for contactless access control. It offers a hygienic, intuitive, and secure method of identity authentication, particularly in environments where users may prefer not to touch shared surfaces or where higher assurance is required.

Armatura's palm technology uses a bi-modal approach. It combines palm shape authentication with visible light and palm vein authentication with infrared light. According to the uploaded Armatura material, visible-light palm authentication analyzes external palm characteristics such as volume, curvature, and finger positions, while infrared palm vein authentication captures vein patterns beneath the palm's surface that are not visible to the naked eye.

This combination is important because each modality contributes different strengths. Visible-light palm recognition can support convenient contactless acquisition and external palm feature analysis. Infrared palm vein recognition strengthens identity assurance because palm veins are internal biological patterns. The uploaded palm material states that palm vein patterns are relatively stable and are not easily affected by age, environmental factors, general physiological changes, or minor surface injuries.

Bi-modal palm authentication therefore provides a layered recognition model. The system does not rely only on the visible appearance of the hand. It also analyzes internal vein patterns that are more difficult to observe, copy, or reproduce. This increases both security and reliability.

Armatura's palm authentication process includes palm acquisition, palm image standardization, image quality assessment, liveness detection, ROI processing, feature extraction, palm encoding, and matching. The uploaded material describes ROI enhancement as a critical process for improving the accuracy and reliability of palm authentication by highlighting distinctive palm characteristics under different environmental or lighting conditions.

After ROI enhancement, the system extracts important palm feature points and converts them into palm codes. These palm codes represent the distinctive characteristics of the palm and are used for comparison against stored templates.

3.4 Palm Liveness Detection and Anti-Spoofing

Palm authentication also requires protection against spoofing attempts. Attackers may attempt to use printed palm images, fake hands, gloves, rubber hands, or palm images displayed on electronic devices. Armatura addresses this risk through palm liveness detection and anti-spoofing analysis.

The uploaded Armatura palm material explains that liveness detection analyzes reflection patterns, material

textures, light distribution, and surface structures to distinguish between genuine palms and spoofed images or objects. It also highlights the importance of infrared palm vein characteristics, which are associated with internal biological patterns that cannot be fully replicated by common spoofing materials.

The palm anti-spoofing process includes image standardization, palm quality assessment, liveness scoring, feature storage across modalities, classifier-based judgment, and final decision fusion. If the palm is determined to be genuine, the system proceeds to palm authentication.

Armatura's dual-modality palm architecture strengthens anti-spoofing because it evaluates both visible and infrared information. A fake palm object may visually resemble a real palm, but it may not reproduce the internal vein characteristics, spectral response, reflection behavior, and liveness-related features expected from a genuine human palm.

3.5 Biometric Template Protection

A biometric system must protect not only the authentication process, but also the biometric data generated during enrollment and recognition. Armatura's biometric architecture is designed to minimize exposure of sensitive biometric information.

The uploaded Armatura irreversibility material explains that after facial or palm images are collected, the system extracts only the necessary biometric features required for authentication and does not store the original images. It further states that the templates are not interpretable and cannot be used to reverse-engineer the complete original biometric images.

This design is important because biometric templates are not treated as raw biometric photographs. Instead, they are mathematical representations derived from selected features. Since unnecessary biometric information is discarded, the stored template is designed to support matching while reducing the risk of reconstructing the original biometric sample.

Armatura also applies encryption to biometric templates and sensitive user information. The uploaded material states that AES-256 encryption is used for biometric templates and that sensitive information such as usernames, user IDs, and user photos is also protected during storage and transmission.

This creates a layered security model:

Layer	Purpose
Data minimization	Collect and retain only what is required for authentication
Feature extraction	Convert biometric images into mathematical features
Template irreversibility	Prevent reconstruction of the original biometric image
Encryption	Protect templates and sensitive user information
Liveness detection	Reduce the risk of spoofing and presentation attacks
Matching control	Compare protected templates for verification or identification

3.6 Unified Value Proposition

Armatura's multimodal biometric technology is designed to deliver a balanced combination of security, convenience, privacy, and scalability.

For users, the system provides fast and contactless authentication. For security teams, it strengthens assurance by linking access events to physical identity. For system integrators, it offers a biometric architecture that can support different deployment scenarios. For enterprise decision-makers, it provides a path toward higher security without creating unnecessary operational friction.

The key value of Armatura biometrics can be summarized as follows:

Capability	Client Value
Face recognition	Fast, natural, contactless authentication
Bi-modal palm authentication	Higher-assurance palm recognition using visible and infrared modalities
Liveness detection	Protection against spoofing and presentation attacks
Deep learning recognition	Robust feature extraction and scalable matching
Irreversible templates	Reduced risk of biometric image reconstruction
AES-256 encryption	Secure storage and transmission of biometric templates and sensitive data
Contactless operation	Improved hygiene, convenience, and user experience
Multimodal flexibility	Adaptable authentication options for different environments and security levels

Armatura's biometric technology should therefore be understood not as a single recognition feature, but as a complete biometric trust architecture. It combines sensing, intelligence, anti-spoofing, secure template processing, and enterprise deployment readiness into a unified access control solution.

This foundation prepares the whitepaper for the next technical sections, where the document will go deeper into the end-to-end authentication architecture, face recognition pipeline, face liveness detection, bi-modal palm recognition, palm anti-spoofing, template irreversibility, and performance validation.

4. End-to-End Biometric Authentication Architecture

Armatura biometric authentication is designed as an end-to-end identity verification architecture rather than a single recognition function. In a modern access control environment, a biometric system must do more than compare one image against another. It must acquire the biometric sample, assess its quality, determine whether the sample is genuine, extract usable biometric features, convert those features into protected templates, perform identity comparison, and return a reliable access decision within a short operational timeframe.

This architecture is built around a complete biometric authentication lifecycle:

Stage	Function	Security Purpose
Biometric acquisition	Captures face, palm, or other biometric input	Establishes the source biometric sample
Preprocessing	Normalizes image size, angle, contrast, noise, and quality	Improves reliability of downstream processing
Quality assessment	Determines whether the sample is suitable for recognition	Reduces false rejection and low-quality matching
Liveness detection	Determines whether the sample is from a genuine live user	Protects against spoofing and presentation attacks
Feature extraction	Extracts distinctive biometric characteristics	Converts images into mathematical identity features
Template generation	Produces compact biometric representation	Supports matching without storing raw biometric images
Template protection	Applies irreversibility and encryption	Reduces privacy and data security risk
Matching	Compares live features with enrolled templates	Supports 1:1 verification and 1:N identification
Access decision	Returns allow, deny, or exception result	Enforces security policy at the access point

Armatura's uploaded irreversibility material describes this process as a sequence beginning with data collection and preprocessing, followed by feature extraction, classification and authentication, and final evaluation or identification. It also states that after facial or palm images are collected, the system extracts only the necessary biometric features for authentication and does not store the original images.

4.1 Biometric Acquisition

The first stage of biometric authentication is acquisition. In this stage, the biometric terminal captures the required biometric sample from the user. Depending on the deployed device and authentication policy, this may include a facial image, visible-light palm image, infrared palm image, fingerprint sample, or a combination of modalities.

For face recognition, image acquisition is typically performed through a camera module that captures the user's face at the access point. For palm authentication, Armatura's bi-modal architecture uses visible-light and infrared palm acquisition. The visible-light channel captures external palm characteristics, while the infrared channel captures palm vein information beneath the skin surface.

The objective of acquisition is not simply to capture an image. The system must capture a biometric input that is clear, correctly positioned, and suitable for further processing. In real-world access control environments, acquisition may be affected by lighting, distance, motion, user posture, sensor angle, environmental conditions, and device installation height. Therefore, acquisition must be supported by preprocessing and quality assessment.

4.2 Preprocessing and Standardization

After acquisition, the biometric sample is normalized into a standard input format for algorithmic processing. This step is critical because biometric recognition must operate consistently even when users present themselves under slightly different conditions.

For face recognition, preprocessing may include detection, cropping, alignment, normalization, and adjustment for variations in pose, scale, and orientation. Armatura's face recognition material describes face alignment as the process of normalizing detected face images into a standard coordinate system so that subsequent recognition

can be more effective.

For palm authentication, preprocessing includes palm detection, keypoint localization, region-of-interest extraction, angle correction, and image enhancement. Armatura's palm materials describe palm image standardization as part of the anti-spoofing and authentication pipeline, including palm detection, image quality judgment, liveness detection, and recognition.

This preprocessing stage provides two important benefits. First, it improves recognition accuracy by reducing irrelevant variation. Second, it improves system stability by ensuring that the downstream neural network receives biometric inputs in a consistent format.

4.3 Quality Assessment

Quality assessment determines whether the captured biometric sample is suitable for authentication. A biometric sample may be rejected or recaptured if it is blurred, overexposed, underexposed, partially occluded, improperly positioned, or otherwise unsuitable for reliable recognition.

In face recognition, quality assessment may consider factors such as face visibility, occlusion, pose, lighting, and image sharpness. In palm authentication, quality assessment may evaluate whether the palm is sufficiently visible, whether the region of interest can be extracted, and whether the palm image contains enough useful texture or vein information for liveness and matching.

Quality assessment is important because not all recognition failures are caused by algorithmic weakness. Many are caused by poor acquisition conditions. By evaluating quality before matching, the system can reduce unnecessary false rejection, improve user experience, and prevent low-quality samples from being treated as valid biometric evidence.

4.4 Liveness Detection Before Recognition

Liveness detection is a core security checkpoint in Armatura's biometric architecture. Before the system completes identity recognition, it must assess whether the submitted biometric sample is likely to originate from a genuine live person.

For face recognition, Armatura's anti-spoofing approach uses visible-light and near-infrared information, feature extraction, liveness scoring, and fusion-based decision-making. The uploaded anti-spoofing material states that the binocular anti-spoofing algorithm trains on paired near-infrared and visible-light face images, extracts features from both modalities, and applies a fusion decision strategy to generate the final probability of liveness. For palm authentication, Armatura's liveness detection evaluates both visible-light and infrared palm inputs. The system analyzes features such as reflection patterns, material textures, light distribution, surface structures, and palm vein characteristics to distinguish genuine palms from spoofed objects or images.

Liveness detection helps protect against presentation attacks such as printed photos, replayed images, 3D facial prosthetics, fake palms, rubber hands, gloves, and palm images displayed on smart devices. In a secure access control system, this layer is essential because the system must authenticate the person, not merely accept a visual representation of the person.

4.5 Feature Extraction

Once the biometric input passes acquisition, preprocessing, quality assessment, and liveness detection, the system extracts biometric features. Feature extraction converts the original biometric sample into a mathematical representation that captures distinctive characteristics needed for identity comparison.

For face recognition, extracted features may represent the spatial, structural, and semantic characteristics of the face. Armatura's deep learning material describes the use of deep neural networks to extract high-dimensional feature representations from aligned face images, with Transformer models commonly employed for this task.

For palm authentication, extracted features may include palm shape, texture, skin characteristics, palmprint information, and palm vein patterns. Armatura's palm material explains that after ROI enhancement, the system extracts important palm feature points and converts them into numerical palm codes for matching.

The output of feature extraction is not a raw image. It is a biometric representation designed for recognition. This distinction is central to Armatura's privacy and security model.

4.6 Template Generation and Protection

After feature extraction, the system generates a biometric template. A template is a compact representation of extracted biometric features used for future comparison. It is not intended to be human-readable, and it should not function as a reconstructable image.

Armatura's irreversibility material states that only a small portion of the original biometric information necessary for authentication is retained, while the rest is discarded. As a result, the templates are not interpretable and cannot be used to reverse-engineer the complete original biometric images.

This approach provides a privacy-oriented architecture. Rather than storing raw biometric images for daily authentication, the system stores relevant biometric feature data required for matching. In addition, Armatura's material states that AES-256 encryption is used to protect biometric templates and other sensitive user information during storage and transmission.

In client-facing terms, this means Armatura biometric authentication is designed around three principles:

Principle	Description
Minimize	Retain only the biometric information required for authentication
Transform	Convert biometric samples into mathematical templates
Protect	Use irreversibility and encryption to reduce exposure risk

4.7 Matching and Identity Decision

The final authentication stage is matching. The live biometric template generated at the point of access is compared against enrolled templates stored in the device, server, or authorized biometric database.

There are two primary matching modes:

Matching Mode	Description	Typical Use Case
1:1 verification	Confirms whether the user matches a claimed identity	User presents ID, card, QR code, mobile credential, or account
1:N identification	Searches the enrolled database to identify the user	User authenticates by face or palm without presenting a credential

In 1:1 verification, the biometric system answers the question: "Is this person the same person as the claimed identity?" In 1:N identification, the system answers: "Who is this person among the enrolled population?"

After matching, the biometric engine returns a similarity score or match result. The access control system then applies the configured threshold, user permission, time zone, access level, anti-passback policy, and other security rules before granting or denying access.

4.8 System-Level Security Logic

Armatura biometric authentication should be understood as a sequence of security gates. Each stage reduces a different category of risk.

Security Gate	Risk Reduced
Quality assessment	Poor image quality and unstable recognition
Liveness detection	Spoofing and presentation attacks
Feature extraction	Direct exposure of raw biometric images
Template irreversibility	Reconstruction of original biometric traits
Encryption	Unauthorized reading of stored or transmitted templates
Matching threshold	False acceptance and unauthorized access
Access control policy	Unauthorized entry despite successful identity recognition

This layered architecture is important because biometric security cannot depend on a single algorithmic decision. A reliable system combines sensor design, AI models, template protection, secure storage, communication security, and policy enforcement.

4.9 Chapter Summary

The Armatura biometric authentication architecture provides a structured, end-to-end approach to secure identity verification. It begins with biometric acquisition and preprocessing, continues through quality assessment and liveness detection, extracts distinctive biometric features, generates protected templates, and completes the process through matching and access control decision-making.

This architecture enables Armatura biometric systems to support secure, contactless, and scalable access control while protecting sensitive biometric information. It also establishes the technical foundation for the next chapters: deep learning face recognition, facial liveness detection, and bi-modal palm recognition.

5. Deep Learning Face Recognition

Face recognition is one of the most widely adopted biometric technologies for modern access control because it is intuitive, contactless, and highly suitable for high-throughput environments. Users do not need to touch a sensor, carry a credential, or remember a PIN. Instead, the system authenticates identity by analyzing the user's facial characteristics and comparing them with enrolled biometric templates.

Armatura's face recognition technology is based on deep learning, enabling the system to automatically learn discriminative facial representations from large volumes of training data. Armatura's technical material defines deep learning-based face recognition as a technology that uses deep neural networks to identify and verify individuals based on facial features, using labeled face images to learn features that distinguish different individuals.

5.1 Role of Deep Learning in Face Recognition

Traditional face recognition methods often relied on manually designed features. These systems attempted to identify specific visual patterns in the face using predefined mathematical rules. While effective in controlled environments, traditional approaches may struggle with changes in lighting, pose, facial expression, image resolution, age, occlusion, and camera angle.

Deep learning changes this model. Instead of manually defining every feature, deep neural networks learn feature representations from data. Multiple layers of the network transform the input image into progressively more abstract representations. Lower layers may detect edges, textures, and local visual patterns, while deeper layers capture higher-level facial structures and identity-specific information.

Armatura's uploaded deep learning material explains that deep learning algorithms automatically learn representations through interconnected layers, with each layer applying mathematical transformations that extract increasingly abstract and complex features.

For access control, this capability is important because real-world face recognition must operate under diverse conditions. Users may approach the terminal from different angles. Lighting may vary by time of day. Faces may be partially occluded. Cameras may be installed at different heights. Deep learning allows the recognition model to learn robust representations that support practical deployment.

5.2 Face Recognition Training Pipeline

The training pipeline is the process by which a face recognition model learns to distinguish individuals. Armatura's face recognition material describes the training pipeline as a series of steps involving dataset collection, preprocessing, feature extraction, encoding, and model optimization.

A client-facing view of the training process can be described as follows:

Training Stage	Description
Data preparation	Collects and prepares face images for training
Face detection	Locates the face within the image
Face alignment	Normalizes face position, scale, and orientation
Feature extraction	Extracts high-dimensional facial representations
Loss optimization	Adjusts model parameters to improve recognition performance
Model validation	Tests model behavior against known identity labels

The objective of training is to produce a recognition model that maps images of the same person close together in feature space and separates images of different people. In practical terms, the model learns which facial characteristics are stable and identity-relevant, while reducing the influence of environmental noise or presentation variation.

5.3 Face Recognition Inference Pipeline

Inference is the real-time recognition process used during daily access control operation. During inference, a user presents their face to the terminal, and the system performs detection, anti-spoofing, alignment, feature extraction, matching, and decision-making.

Armatura's material describes the inference pipeline as a sequence consisting of face detection, face

anti-spoofing, face alignment, face feature extraction, and face embedding/matching. It further explains that the extracted face features are compared with templates stored in the machine, and that large-volume comparison may involve database classification.

The process can be described in more formal whitepaper language as follows:

Step 1: Face Detection

The system detects whether a face is present in the image or video frame and determines its position. Detection is the entry point of the face recognition pipeline because all subsequent steps depend on accurate localization of the face.

Step 2: Face Anti-Spoofing

The system evaluates whether the presented face is likely to be from a genuine live person. This stage protects against presentation attacks before recognition is completed.

Step 3: Face Alignment

The detected face is normalized into a consistent coordinate structure. Alignment reduces the impact of head pose, distance, orientation, and scale variation.

Step 4: Face Feature Extraction

The aligned face image is processed by deep neural networks to extract high-dimensional facial features. These features represent identity-relevant characteristics.

Step 5: Face Embedding and Matching

The extracted features are converted into a face embedding and compared against enrolled templates. The system generates a similarity score or identity result, which is then used by the access control system to determine whether access should be granted.

This pipeline allows Armatura face recognition to operate as a structured authentication process, combining recognition accuracy with anti-spoofing and secure identity decision-making.

5.4 Face Embeddings and Template Matching

A face embedding is a mathematical representation of facial features. It is designed to preserve identity-relevant information while reducing the original image into a compact format suitable for matching.

In access control, the embedding generated during authentication is compared with stored templates. If the similarity score meets or exceeds the configured threshold, the system determines that the presented face matches the enrolled identity. If the score is below the threshold, the system rejects the match or requests an alternative authentication method.

Face embeddings support both 1:1 verification and 1:N identification. In 1:1 verification, the live embedding is compared against a specific claimed identity. In 1:N identification, the live embedding is searched against a population of enrolled users.

The advantage of embedding-based recognition is scalability. Armatura's deep learning material notes that face embeddings provide compact and efficient representations, making it feasible to compare and match large numbers of faces in real-time applications.

5.5 Transformer-Based Visual Modeling

Armatura's face recognition technology materials include Transformer-based visual modeling. Transformer architectures are significant in computer vision because they use self-attention mechanisms to model relationships across different regions of an image.

Armatura's material explains that the Transformer uses a hierarchical structure and self-attention mechanisms to capture local and global dependencies in visual data. It divides the input image into smaller patches and applies self-attention operations to model relationships between those patches.

In face recognition, this is valuable because identity is not determined by a single facial region. The model must understand the relationship between eyes, brows, nose, mouth, cheeks, forehead, and overall facial geometry. Self-attention allows the model to focus on different facial regions and learn broader structural relationships. Armatura's Transformer material describes four main parts of the model:

Component	Function
Patch + position embedding	Divides the image into patches and preserves spatial order
Linear projection	Converts patches into vector representations
Transformer encoder	Models relationships between image regions
Face embedding	Produces the final identity representation

The use of Transformer-based modeling supports robust facial representation by capturing both local detail and global facial structure.

5.6 Distortion-Invariant Face Recognition

In real deployments, camera lenses and installation conditions may introduce distortion. Wide-angle cameras, surveillance environments, and non-ideal installation angles can alter the appearance of the face. A recognition system that is too sensitive to such distortion may experience reduced accuracy.

Armatura's material identifies distortion-invariant face recognition as one of its training concepts. It describes a method intended to reduce the effects of radial lens distortion, using an end-to-end approach that can learn rectification, alignment parameters, and face embeddings.

In practical terms, distortion-invariant training helps the recognition model maintain stability when the captured facial image is affected by optical or geometric distortion. This is important for access control systems deployed across different terminal models, camera positions, and installation environments.

5.7 Masked and Occluded Face Recognition

Face recognition performance can be affected when parts of the face are covered or occluded. Occlusion may occur because of masks, sunglasses, scarves, hands, helmets, hats, shadows, or other environmental factors.

Armatura's material describes masked face recognition as an approach that addresses occlusion by recovering occluded facial parts, removing corrupted features, and introducing dynamic random occlusions such as sunglasses, scarves, face masks, hands, eye masks, and eyeglasses during training.

For access control, occlusion handling is important because users may not always present a fully visible face. A robust system should identify when recognition is possible, when the sample quality is insufficient, and when alternative authentication should be requested.

This does not mean that all occluded faces should always be accepted. Instead, the system should be capable of making a controlled decision based on the quality of available biometric evidence, the configured security threshold, and the risk level of the access point.

5.8 Advantages of Deep Learning Face Recognition for Access Control

Armatura's deep learning-based face recognition offers several technical and operational advantages:

Advantage	Description
Contactless authentication	Users can authenticate without touching a sensor
Fast user experience	Suitable for high-throughput entry scenarios
Feature learning	Deep learning extracts identity features automatically
Robustness	Training can improve performance across pose, lighting, and occlusion variation
Scalability	Embeddings support large-scale matching
Integration readiness	Face recognition can work with terminals, access controllers, software platforms, and identity databases

From a security architecture perspective, the value of face recognition is strongest when combined with liveness

detection, template protection, and access control policy enforcement. Recognition alone identifies similarity. A secure biometric access control system must also validate liveness, protect templates, and apply permission rules.

5.9 Chapter Summary

Armatura deep learning face recognition provides a contactless and intelligent method for access control authentication. The technology uses deep neural networks to detect faces, align images, extract high-dimensional features, generate face embeddings, and compare those embeddings with enrolled templates. By incorporating Transformer-based feature modeling, distortion-invariant training, masked-face robustness, and anti-spoofing checks, Armatura face recognition is positioned as a practical biometric foundation for modern access control environments. The next chapter expands on one of the most critical security layers in this architecture: facial liveness detection and anti-spoofing.

same material states that only a portion of the original biometric information required for authentication is retained, while unnecessary information is discarded, making the resulting templates non-interpretable and not usable for reconstructing the complete biometric image.

6. Facial Liveness Detection and Anti-Spoofing

Face recognition systems must defend against presentation attacks. A presentation attack occurs when an attacker presents a fake or manipulated biometric artifact to the system in an attempt to impersonate a legitimate user. Examples include printed photos, digital screen replays, videos, masks, prosthetics, and other artificial representations of a face.

Facial liveness detection, also known as face anti-spoofing, is the process of determining whether the face presented to the system is from a genuine live person. In a high-security access control environment, liveness detection is not optional. It is an essential layer that protects the recognition system from being deceived by non-live biometric samples.

Armatura's anti-spoofing material states that anti-spoofing face recognition is essential for the security of facial recognition systems and that spoofing involves presenting forged or manipulated biometric data to deceive the system. The same material explains that anti-spoofing techniques use advanced algorithms and machine learning models to analyze face characteristics such as texture, motion, depth, and liveness.

6.1 Threat Model for Face Presentation Attacks

A secure biometric system should be evaluated not only by how accurately it recognizes enrolled users, but also by how effectively it rejects fraudulent biometric presentations.

Common face presentation attack instruments include:

Attack Type	Description
Printed photo	A printed image of an authorized user's face
Screen replay	A face image or video displayed on a phone, tablet, or monitor
Cut-out image	A printed face image with cut-out regions intended to simulate depth
3D mask	A mask designed to reproduce facial shape and appearance
Facial prosthetic	Artificial material placed over part or all of the face
Partial occlusion attack	A presentation that combines real and artificial facial regions
Makeup or disguise	Attempt to alter or imitate facial characteristics

Armatura's face anti-spoofing materials specifically identify attack categories such as color-printed paper, cut-out printed paper, 3D facial prosthetics, partially occluded prosthetics, and fully occluded prosthetics.

The objective of facial liveness detection is to distinguish a live human face from these artificial or manipulated presentations before the recognition result is accepted.

6.2 Multimodal Face Anti-Spoofing

Armatura's facial anti-spoofing approach uses a binocular architecture based on visible-light and near-infrared facial inputs. The system analyzes both modalities and applies a fusion strategy to produce a liveness result.

Visible-light imaging captures facial appearance, texture, color, and surface characteristics. Near-infrared imaging provides additional spectral information that can help distinguish live facial tissue from printed or artificial materials. By combining the two, the system can evaluate a broader range of liveness cues than a single image channel alone.

Armatura's anti-spoofing material states that, during training, the binocular anti-spoofing algorithm uses paired near-infrared and visible-light face images. Deep neural networks extract features from both image types, including shallow-level characteristics such as shape, texture, reflection, and spectrum, as well as deep semantic features. During inference, the algorithm takes binocular face pairs from dual cameras, performs liveness assessment on each modality, and fuses the results into a final liveness probability.

6.3 Facial Anti-Spoofing Training

The purpose of anti-spoofing training is to teach the model to separate genuine live faces from spoofing attacks across different conditions and attack materials.

The training process uses both live and attack samples. The model learns how genuine faces appear across visible-light and near-infrared channels, and it also learns the patterns commonly associated with spoofing

media. These may include flat texture, abnormal reflection, inconsistent depth behavior, artificial surface structure, lack of natural skin response, or differences between visible-light and infrared appearance.

Armatura's face recognition material states that during the algorithm training phase, real face images are included together with 3D masks, fake photos, and partial fake photos. The anti-spoofing machine learning process evaluates the loss function of the input image to differentiate between real and fake images.

In a formal technical architecture, this process can be described through four training objectives:

Training Objective	Description
Learn live-face characteristics	Model genuine face appearance across modalities
Learn spoof-material characteristics	Identify features associated with printed, digital, or prosthetic attacks
Optimize decision boundaries	Separate live and spoof samples in feature space
Improve cross-condition robustness	Maintain performance across lighting, pose, device, and user variation

The result is a liveness classifier that supports real-time anti-spoofing judgment during authentication.

6.4 Facial Anti-Spoofing Inference Workflow

During daily operation, facial liveness detection is performed as part of the recognition pipeline. The system first captures the face, standardizes the image, evaluates quality, performs liveness analysis, and then allows recognition to continue only if the liveness result meets the configured threshold.

Armatura's anti-spoofing material describes the workflow as follows: obtain standardized face images through face detection, apply face occlusion recognition and face quality assessment, store different modal features and predict liveness scores, use a trained face liveness classifier for classification, fuse the binocular inference results, and proceed to face recognition only if the prediction indicates liveness.

For whitepaper purposes, the workflow can be expressed as:

Step 1: Face Acquisition and Detection
The terminal captures facial input and detects the face region.

Step 2: Standardization and Quality Assessment
The face is normalized into the model input format. The system evaluates whether the captured face is suitable for reliable analysis.

Step 3: Occlusion and Spoofing Analysis
The system evaluates whether the face is obstructed, artificially modified, or visually inconsistent with a live presentation.

Step 4: Multimodal Feature Extraction
Visible-light and near-infrared features are extracted and stored in feature units for liveness prediction.

Step 5: Liveness Score Generation
Each modality produces a liveness score, and the multimodal feature representation may also produce a fused score.

Step 6: Fusion Decision
The system combines the liveness judgments from visible-light, near-infrared, and multimodal analysis.

Step 7: Recognition Continuation or Rejection
If the system determines that the input is live, the face recognition process continues. If the liveness result is insufficient, authentication is rejected or an alternative method is requested.

6.5 Liveness Features and Decision Cues

A robust face anti-spoofing system evaluates multiple characteristics. No single cue is sufficient in all environments because attack methods vary. A printed image may look realistic in visible light but lack depth. A digital replay may display a face but produce abnormal reflection. A 3D mask may have shape but fail spectral or

texture-based analysis.

Armatura's material describes anti-spoofing analysis using reflection patterns, materials, textures, light distributions, and surface structures. These cues allow the system to evaluate whether the presented face behaves like a live face or an artificial object.

Liveness Cue	Security Relevance
Texture	Detects abnormal print, screen, or material patterns
Reflection	Identifies artificial surface behavior
Spectrum	Compares visible-light and near-infrared characteristics
Depth or 3D structure	Helps distinguish flat media from real faces
Occlusion	Detects blocked, modified, or partially fake facial regions
Multimodal consistency	Verifies that visible and infrared evidence support the same live-face conclusion

The combination of these cues strengthens resistance against different attack types.

6.6 Relationship Between Anti-Spoofing and Recognition

Facial liveness detection and face recognition serve different purposes.

Face recognition answers: "Whose face is this?"

Facial liveness detection answers: "Is this a genuine live face?"
Both are required for secure biometric access control. A system may recognize a printed photo as visually similar to an enrolled user, but liveness detection should prevent the authentication event from being accepted. Similarly, a live person may be present, but if the face does not match an enrolled template, recognition should reject the authentication.

Therefore, the secure authentication decision depends on both identity confidence and liveness confidence.

Condition	Result
Live + identity match	Access may proceed, subject to permission policy
Live + no identity match	Access denied
Spoof + identity match	Access denied
Spoof + no identity match	Access denied
Poor quality	Recapture or fallback authentication

This layered decision logic helps ensure that Armatura face recognition is not only accurate, but also resistant to intentional impersonation attempts.

6.7 Client Benefits of Facial Anti-Spoofing

For enterprise and high-security clients, facial liveness detection provides several direct benefits:

Benefit	Client Impact
Reduced impersonation risk	Helps prevent unauthorized access using fake biometric media
Higher trust in access logs	Increases confidence that recorded access events correspond to live users
Stronger biometric assurance	Adds security beyond image similarity matching
Better deployment suitability	Supports use in higher-risk access points
Improved compliance posture	Supports responsible biometric security design

In practical deployment, facial anti-spoofing is especially important for locations such as corporate headquarters, data centers, R&D laboratories, airports, financial institutions, healthcare facilities, and critical infrastructure sites.

6.8 Chapter Summary

Facial liveness detection is a core security function in Armatura's biometric access control architecture. It protects face recognition from presentation attacks by analyzing whether the submitted biometric sample is from a

genuine live person.

Armatura's approach combines visible-light and near-infrared input, deep neural network feature extraction, liveness scoring, multimodal fusion, face quality assessment, and analysis of spoofing indicators such as reflection, texture, material, light distribution, and surface structure.

By placing liveness detection before final recognition, Armatura strengthens the trustworthiness of face-based authentication and provides a more secure foundation for enterprise access control.

7. Bi-Modal Palm Recognition Technology

Bi-modal palm recognition is a key component of Armatura's multimodal biometric architecture. It provides a contactless and high-assurance authentication method by combining two palm-based modalities: visible-light palm recognition and infrared palm vein recognition.

Armatura's palm technology is designed to capture both external and internal palm characteristics.

Visible-light palm recognition analyzes features visible on the surface of the hand, such as palm shape, texture, curvature, and finger positions. Infrared palm vein recognition captures vein patterns beneath the skin surface, which are not visible to the naked eye. Armatura's material describes bi-modal palm authentication as the combination of these two modalities to enhance the accuracy and stability of contactless biometric authentication.

7.1 Why Palm Recognition Matters

Palm recognition offers several advantages for access control. It is contactless, intuitive, hygienic, and suitable for users who may not want to touch shared devices. It also provides a broad biometric surface, allowing the system to analyze multiple identity-related characteristics from the hand.

Compared with some other biometric modalities, palm authentication can be more comfortable for users in public or semi-public access control scenarios. Users can present their palm naturally in front of the terminal without physical contact. This makes palm authentication suitable for corporate entrances, turnstiles, clean environments, hospitals, laboratories, schools, factories, and high-security access points.

The security value of palm recognition becomes stronger when external palm features are combined with internal vein patterns. External characteristics help support convenient recognition, while internal vein structures provide an additional layer of biological uniqueness and anti-spoofing strength.

7.2 Two Modalities in Armatura Palm Authentication

Armatura's bi-modal palm recognition uses two complementary channels.

Modality	Input Type	Biometric Characteristics
Visible-light palm recognition	Visible-light palm image	Palm shape, texture, curvature, skin features, finger position
Infrared palm vein recognition	Infrared palm image	Vein distribution and internal palm vein patterns

Visible-light palm authentication uses visible-light cameras or sensors to capture palm images or videos. The system identifies the user by analyzing characteristics such as palm shape, texture, and skin features. Infrared palm authentication captures infrared images of the palm and analyzes vein distribution and vein patterns beneath the skin.

The purpose of combining these modalities is to produce a more comprehensive biometric representation than either modality alone. Visible-light palm recognition contributes external morphology and texture information. Infrared palm vein recognition contributes internal vascular structure information.

7.3 Visible-Light Palm Recognition

Visible-light palm recognition analyzes the external features of the palm. These may include the overall palm shape, hand geometry, finger position, surface texture, palm lines, and skin appearance.

This modality is valuable because it supports contactless authentication at a practical distance and can capture visually accessible features quickly. It contributes to user convenience and operational speed, especially in access control scenarios where many users must authenticate efficiently.

However, visible-light features alone may be more exposed to environmental variation and spoofing attempts. Lighting conditions, hand angle, surface appearance, and image quality can affect the visible-light image. Therefore, Armatura combines visible-light palm recognition with infrared palm vein recognition to strengthen the overall authentication decision.

7.4 Infrared Palm Vein Recognition

Infrared palm vein recognition captures vein patterns beneath the surface of the palm. These vein patterns are internal biological characteristics and are not visible to the naked eye.

Armatura's palm authentication material explains that infrared light has a longer wavelength and higher penetration power than visible light, enabling it to penetrate skin tissue and reach the deeper vein network. The system analyzes the vein distribution and patterns in infrared palm images for identification and authentication. The same material states that palm vein patterns are relatively stable and are not generally affected by age, environmental factors, general physiological changes, or minor surface injuries.

This gives palm vein recognition strong value for high-security authentication. Because the vein pattern is internal, it is more difficult to observe, capture, copy, or reproduce than surface-level biometric features. When used together with visible-light palm recognition, it strengthens both identity assurance and anti-spoofing capability.

7.5 Cross-Modal Fusion

The most important technical principle of Armatura bi-modal palm recognition is cross-modal fusion. The system captures both visible-light and infrared palm images, extracts features from both modalities, and integrates the information into a more complete representation.

Armatura's material states that bi-modal palm authentication captures both visible-light and infrared palm images and uses advanced algorithms for cross-modal fusion, integrating and complementing the data from both modalities to obtain a more comprehensive and accurate analysis.

Cross-modal fusion allows the system to evaluate the palm from two perspectives:

Perspective	Contribution
External palm morphology	Supports convenient acquisition and surface-level identity features
Internal palm vein structure	Strengthens security, uniqueness, and liveness evidence

The result is a palm authentication process designed to provide both usability and security.

7.6 Palm Authentication Pipeline

Armatura's palm authentication pipeline can be described as a sequence of acquisition, preprocessing, quality assessment, liveness detection, ROI enhancement, feature extraction, palm encoding, and matching.

Step 1: Palm Acquisition
The terminal captures visible-light and infrared palm images.

Step 2: Palm Detection and Keypoint Localization
The system detects the palm and identifies keypoints that help determine palm position, orientation, and region of interest.

Step 3: Image Quality Assessment
The system determines whether the palm image is clear and suitable for liveness and recognition processing.

Step 4: Region of Interest Extraction and Enhancement
The system isolates the important palm region and enhances relevant features.

Step 5: Liveness Detection
The system evaluates whether the palm input is from a genuine live palm or a spoofing object.

Step 6: Feature Extraction
The system extracts palm shape, texture, palmprint, and vein-related features.

Step 7: Palm Encoding
Extracted features are converted into palm codes or mathematical feature representations.

Step 8: Matching
The live palm code is compared with enrolled templates to verify or identify the user.

Armatura's palm anti-spoofing workflow also describes a sequence of palm keypoint detection, palm ROI acquisition, palm quality assessment, palm liveness detection, and palm recognition.

7.7 Region of Interest Enhancement

Region of Interest, or ROI, enhancement is a critical stage in palm authentication. The full palm image may contain irrelevant background, inconsistent lighting, or areas that do not contribute meaningfully to recognition. ROI processing isolates the most useful palm region and improves the quality of biometric analysis.

Armatura's material explains that ROI enhancement improves the accuracy and reliability of palm authentication by adjusting contrast, brightness, sharpness, and other image characteristics so that unique palm features can be highlighted under different environmental or lighting conditions.

ROI enhancement supports recognition in three ways:

Function	Benefit
Focus	Directs the algorithm to the most identity-relevant palm area
Enhancement	Improves visibility of palm texture and vein-related features
Robustness	Reduces the impact of background and environmental variation

This step is particularly important in contactless authentication, where hand position, angle, and distance may vary between users.

7.8 Palm Encoding and Matching

After ROI enhancement and feature extraction, the system converts palm characteristics into palm codes. These codes are mathematical representations used for comparison.

Armatura's palm material states that after ROI enhancement, the system extracts important feature points from the palm image and converts them into specific numerical values called palm codes. These codes may be based on palm texture, shape, skin features, and other characteristics. Palm matching then compares the captured user's palm code with stored palm codes to identify the individual.

Palm encoding provides the technical bridge between biometric acquisition and identity matching. The system does not need to compare raw images directly. Instead, it compares structured feature representations generated from the live palm sample and enrolled templates.

7.9 Palm Augmentation and Training Robustness

Palm recognition must operate across different users, hand positions, lighting conditions, skin characteristics, image qualities, and environmental variables. To improve robustness, Armatura's training approach includes palm augmentation and synthetic palm image generation.

Palm augmentation refers to processing palm images to extract useful features, eliminate interference factors, and improve image clarity. Armatura's palm material states that palm augmentation addresses challenges caused by lighting, angle, positioning, diversity, and complexity of palm images, using techniques such as image enhancement, feature extraction, pose correction, and segmentation.

Synthetic palm image generation further expands training diversity. Armatura's material explains that synthetic palm images can simulate angles, poses, environmental conditions, lighting variations, blur, noise, and partial occlusion. It also states that the system uses StyleGAN-based generation and an ID uniqueness discriminator to evaluate whether generated synthetic palm images are sufficiently unique before they are included in the training dataset.

This improves model adaptability by exposing the training process to a wider range of possible palm appearances and capture conditions.

7.10 Advantages of Bi-Modal Palm Recognition

Armatura bi-modal palm recognition provides several advantages for access control:

Advantage	Explanation
Contactless authentication	Users authenticate without touching a shared surface
Enhanced accuracy	Visible-light and infrared features complement each other
Stronger security	Internal palm vein patterns add a difficult-to-replicate biometric layer
Improved stability	Palm vein patterns are internal and relatively stable
Anti-spoofing support	Liveness analysis can evaluate both surface and infrared characteristics
User convenience	Palm presentation is natural and easy to understand
Deployment flexibility	Suitable for corporate, commercial, institutional, and high-security environments

Armatura's palm material emphasizes enhanced accuracy, superior anti-spoofing capability, contactless authentication, and convenient authentication as key advantages of its bi-modal palm approach.

7.11 Use Cases for Bi-Modal Palm Authentication

Bi-modal palm recognition is suitable for environments where organizations require contactless user experience and stronger biometric assurance.

Typical use cases include:

Environment	Value of Palm Authentication
Corporate headquarters	Fast and hygienic staff access
Data centers	High-assurance access to sensitive infrastructure
Laboratories	Contactless access where hygiene and security matter
Healthcare facilities	Reduced surface contact and controlled staff access
Schools and campuses	Convenient identity authentication for large user groups
Industrial sites	Practical authentication where cards may be inconvenient
Airports and transport facilities	High-throughput, contactless identity verification
Smart buildings	Integrated biometric access for modern property management

Palm authentication can also serve as a strong alternative or complement to face recognition. In environments where users prefer not to use face recognition, or where face recognition may be affected by masks, helmets, or lighting, palm authentication provides an additional biometric pathway.

7.12 Chapter Summary

Armatura bi-modal palm recognition combines visible-light palm recognition and infrared palm vein recognition into a unified authentication architecture. Visible-light palm recognition supports convenient contactless acquisition and external palm feature analysis. Infrared palm vein recognition adds internal biological characteristics that strengthen stability, uniqueness, and security.

Through cross-modal fusion, ROI enhancement, palm encoding, liveness detection, palm augmentation, and synthetic training data, Armatura palm authentication is designed to provide a secure and practical biometric method for modern access control.

This chapter establishes the technical foundation for the next section of the whitepaper: palm liveness detection and anti-spoofing, where the system's resistance to fake palms, printed images, gloves, rubber hands, and screen-based attacks will be discussed in greater detail.

8. Palm Liveness Detection and Anti-Spoofing

Palm recognition provides strong biometric assurance, especially when visible-light palm recognition is combined with infrared palm vein recognition. However, like all biometric systems, palm authentication must be protected against presentation attacks. A presentation attack occurs when an attacker attempts to deceive the biometric system by presenting an artificial or copied biometric object instead of a genuine live human biometric trait.

For palm authentication, potential spoofing media may include printed palm images, grayscale palm prints, palm images displayed on mobile screens, gloves, fake hands, rubber hands, or other artificial hand-like objects. A secure palm authentication system must therefore determine not only whether a presented palm matches an enrolled user, but also whether the presented palm is genuine and live.

Armatura's palm liveness detection architecture is designed to address this challenge through a combination of visible-light analysis, infrared palm vein analysis, feature-level liveness classification, and fusion-based decision-making. The system evaluates characteristics such as reflection patterns, material textures, light distribution, surface structures, and palm vein properties to distinguish genuine palms from spoofed objects or images.

8.1 Threat Model for Palm Presentation Attacks

A palm presentation attack attempts to imitate the biometric appearance of an authorized user's hand. Unlike simple card theft or PIN sharing, biometric spoofing attempts to exploit the recognition algorithm itself. This makes liveness detection a critical layer in biometric access control.

Typical palm presentation attack instruments include:

Attack Type	Description	Security Risk
Color-printed palm image	A printed image of an authorized user's palm	May attempt to imitate visible palm texture
Grayscale or black-and-white print	A monochrome printed palm image	May target systems that rely only on surface pattern
Palm image on smart device	A palm displayed on a phone, tablet, or screen	May simulate a live presentation visually
Gloved hand	A glove or covering designed to imitate palm features	May attempt to bypass surface-feature analysis
Fake hand or rubber hand	Artificial hand-like object	May attempt to imitate physical hand shape
Partial spoof object	A combination of real hand and artificial surface	May attempt to confuse liveness and matching stages

Armatura's uploaded palm anti-spoofing material specifically identifies spoofing examples including color-printed paper, black-and-white printed paper, fake palm prints with gloves, fake hands or rubber hands, and palm prints on smart devices.

The goal of palm liveness detection is to reject these attack instruments before the system proceeds to a successful authentication decision.

8.2 Why Bi-Modal Palm Improves Anti-Spoofing

Single-modality palm recognition may depend heavily on visible palm appearance. While visible-light recognition can provide fast and convenient acquisition, visible surface characteristics may be easier to imitate than internal biological structures. Armatura's bi-modal approach strengthens security by combining visible-light palm recognition with infrared palm vein recognition.

Visible-light palm recognition analyzes external palm features such as palm shape, texture, curvature, volume, and finger positions. Infrared palm vein recognition captures internal vein patterns beneath the skin surface, which are not visible to the naked eye. Armatura's palm material states that infrared light can detect blood circulation in veins and that palm veins are located inside the body, making them difficult to observe or replicate. This bi-modal design improves anti-spoofing in two ways.

First, it gives the system more evidence. A spoof object may imitate the external appearance of a palm, but it is

significantly more difficult to reproduce the internal vein structure and infrared spectral response of a live hand.

Second, it allows cross-modal consistency checking. A genuine palm should present consistent identity and liveness evidence across visible-light and infrared channels. If the visible image appears palm-like but the infrared channel does not show expected vein-related liveness characteristics, the system can reject the presentation.

8.3 Palm Liveness Detection Cues

Armatura palm liveness detection analyzes multiple physical and visual characteristics. This multi-cue strategy is important because spoofing methods vary. A printed image, a screen replay, a glove, and a rubber hand may fail in different ways. A robust anti-spoofing system should therefore evaluate several types of evidence rather than relying on one signal alone.

Liveness Cue	Purpose
Reflection pattern	Detects abnormal reflection behavior from paper, screens, rubber, or synthetic materials
Material texture	Identifies texture differences between live skin and artificial objects
Light distribution	Evaluates how light interacts with the presented palm surface
Surface structure	Helps distinguish real biological skin from printed or artificial surfaces
Infrared vein response	Verifies internal palm vein characteristics beneath the skin
Cross-modal consistency	Confirms that visible-light and infrared evidence support the same live-palm conclusion

Armatura's material states that palm liveness detection analyzes reflection patterns, material textures, light distribution, and surface structures, and uses these signals to distinguish real palms from disguised palm images or objects.

8.4 Palm Anti-Spoofing Training Architecture

Armatura's palm anti-spoofing training process uses deep neural networks to learn the difference between genuine palm presentations and spoofing samples. During training, palm images from different data domains are transformed into a standardized model input format. The system then uses a dual-branch network to extract and decouple features.

One branch preserves the original resolution of the palm image and extracts original features. Another branch uses an attention module to decouple domain-style features and liveness-content features. Domain-style features may include palm shape, texture, and reflection in visible-light images, while liveness-content features may include palm vein structure and texture in infrared images.

This design is important because palm anti-spoofing must generalize across different users, environments, devices, and spoofing materials. A system that works only against one attack type is not sufficient for enterprise access control. The training architecture must help the model learn generalized liveness characteristics rather than memorizing a narrow set of examples.

Armatura's material further explains that enhanced feature sets are synthesized and combined with original image features to train the palm image classifier, improving palm identification and anti-spoofing performance across different data domains.

8.5 Palm Anti-Spoofing Inference Workflow

During operation, palm liveness detection is performed before the final recognition decision. The workflow can be described as follows:

Step 1: Palm Acquisition
The terminal captures palm images through visible-light and infrared channels.

Step 2: Palm Detection and Standardization
The palm is detected and converted into a standardized model input format.

Step 3: ROI Acquisition
The system extracts the region of interest from the palm image, focusing on the areas most relevant to authentication.

Step 4: Palm Quality Assessment
The system checks whether the palm image is suitable for liveness detection and recognition.

Step 5: Palm Liveness Detection
The system extracts visible-light and infrared features, predicts liveness scores, and applies a trained liveness classifier.

Step 6: Fusion Decision
The system fuses the inference results from binocular or dual-modal images to generate a final palm liveness result.

Step 7: Palm Recognition
If the palm is determined to be live, the system proceeds to palm recognition and matching.

Armatura's uploaded palm technology material describes this workflow as palm keypoint detection, palm ROI acquisition, palm quality assessment, palm liveness detection, and palm recognition. It also states that the system uses different modal features, predicts corresponding liveness scores, and fuses the inference results to generate the final palm prediction result.

8.6 Relationship Between Palm Liveness and Palm Recognition

Palm liveness detection and palm recognition are related but separate functions.

Palm recognition answers: "Whose palm is this?"

Palm liveness detection answers: "Is this a genuine live palm?"

A secure biometric decision requires both answers. If the palm matches an enrolled user but fails liveness detection, access should be denied. If the palm is live but does not match an authorized user, access should also be denied. Only when the palm is both live and matched to an authorized identity should the access control system proceed to policy evaluation.

Liveness Result	Recognition Result	Authentication Outcome
Live	Match	Access may proceed, subject to access policy
Live	No match	Access denied
Spoof	Match-like similarity	Access denied
Spoof	No match	Access denied
Poor quality	Unknown	Recapture or fallback authentication

This layered logic prevents the system from treating biometric similarity alone as sufficient proof of identity.

8.7 Client Benefits of Palm Anti-Spoofing

Palm anti-spoofing provides direct value for enterprise clients and high-security projects.

Benefit	Client Value
Higher resistance to spoofing	Helps reject printed images, screen replays, gloves, fake hands, and rubber hands
Stronger identity assurance	Confirms both palm identity and live biological presentation
Improved trust in access events	Supports more reliable audit trails and access records
Contactless security	Delivers secure authentication without physical contact
Better suitability for sensitive sites	Supports deployment in corporate, industrial, healthcare, laboratory, and critical environments

For clients evaluating biometric access control, palm liveness detection is a key differentiator. It transforms palm recognition from a visual matching function into a high-assurance authentication process.

8.8 Chapter Summary

Armatura palm liveness detection and anti-spoofing provide a critical security layer for bi-modal palm authentication. By combining visible-light palm analysis, infrared palm vein analysis, feature-level liveness

scoring, material and reflection analysis, and fusion-based decision-making, the system is designed to reject spoofing attempts before recognition is completed.

This approach strengthens the security value of Armatura's palm authentication technology and supports reliable contactless access control in modern enterprise environments.

9. Biometric Template Irreversibility and Data Protection

Biometric authentication depends on sensitive biological characteristics. For this reason, a biometric access control system must be designed not only for recognition accuracy, but also for privacy, data minimization, template protection, and secure system operation. Clients need confidence that biometric data is handled responsibly throughout the entire authentication lifecycle.

Armatura's biometric architecture is designed around a privacy-first principle: biometric images are used to extract necessary features for authentication, while the complete original biometric images are not stored for routine matching. The uploaded Armatura irreversibility material states that after collecting facial or palm images, the system extracts only the necessary biometric features required for authentication and does not store the original images, reducing the risk of image theft.

9.1 Why Biometric Template Protection Matters

Biometric data differs from traditional credentials. A password can be reset. A card can be replaced. A PIN can be changed. A face, palm, or fingerprint cannot be changed in the same way. Therefore, biometric systems must be designed to reduce the exposure of biometric data and protect the mathematical templates used for authentication.

A secure biometric system should address the following risks:

Risk	Description
Raw image exposure	Unauthorized access to facial, palm, or fingerprint images
Template theft	Unauthorized extraction of biometric templates
Template reconstruction	Attempt to recover original biometric traits from stored templates
Unauthorized matching	Improper use of templates outside the intended system
Data interception	Capture of biometric data during transmission
Excessive data retention	Storage of biometric information beyond operational need

Armatura's template protection strategy addresses these risks through feature extraction, data minimization, irreversibility, and encryption.

9.2 From Biometric Image to Biometric Template

The biometric authentication process begins with biometric acquisition. The system captures a face or palm image at the terminal. However, the purpose of this capture is not to create a stored image archive. The purpose is to extract the biometric features needed for authentication.

Armatura's uploaded material describes the process as follows: the system collects necessary biometric data, preprocesses it by resizing, adjusting angles, enhancing contrast, and removing noise, then extracts useful features such as textures, shapes, and edges using deep learning models.

During feature extraction, only a portion of the biometric information needed for authentication is retained. Unnecessary information is discarded. The retained data becomes a biometric template or feature representation used for future comparison.

This architecture provides a key privacy benefit: the system does not depend on storing the complete raw biometric image for every future authentication event.

9.3 Template Irreversibility

Template irreversibility means that a biometric template cannot be used to reconstruct the original biometric image. In Armatura's architecture, the template is designed as a mathematical representation of selected biometric features, not as a reversible image file.

The uploaded Armatura irreversibility document states that only a small portion of the original biometric information necessary for authentication is retained, while the rest is discarded and not stored. As a result, the templates are not interpretable and cannot be used to reverse-engineer the original biometric images. It further states that neither Armatura nor a third party can reconstruct the complete biometric images from these templates.

For a client-facing whitepaper, this point should be communicated carefully and clearly. The message should not be that biometric data has no sensitivity. The message should be that Armatura's architecture is designed to reduce biometric data exposure by avoiding routine storage of reconstructable raw images and by converting biometric features into protected templates.

9.4 Data Minimization

Data minimization is the practice of collecting and retaining only the data necessary for a defined purpose. In biometric access control, the defined purpose is authentication. Therefore, the system should avoid storing unnecessary biometric images or redundant biological information.

Armatura's material states that the system extracts only the necessary biometric features for authentication and does not store facial or palm images after feature extraction.

This supports a privacy-by-design architecture:

Principle	Armatura Design Approach
Purpose limitation	Biometric data is processed for authentication
Data minimization	Only required biometric features are retained
Storage limitation	Raw biometric images are not stored for routine matching
Security by design	Templates are protected through irreversibility and encryption
Controlled processing	Matching is performed using internal template or database comparison

This approach helps clients reduce biometric data risk while still benefiting from biometric access control.

9.5 AES-256 Encryption for Biometric Templates

In addition to irreversibility, Armatura applies encryption to protect biometric templates and other sensitive user information. The uploaded Armatura document states that AES-256 encryption is used for biometric templates to support secure storage and transmission of biometric data. It also states that encryption is extended to other sensitive user information, including usernames, user IDs, and user photos.

Encryption provides protection if stored or transmitted data is intercepted or accessed without authorization. Even if encrypted data is acquired, it cannot be directly read or used without the appropriate cryptographic key.

In a whitepaper, this section should emphasize that encryption is part of a layered protection model, not the only protection method. Armatura combines:

Protection Layer	Function
Raw image non-storage	Reduces exposure of original biometric images
Feature extraction	Converts biometric samples into mathematical features
Template irreversibility	Prevents reconstruction of complete biometric images
AES-256 encryption	Protects templates and sensitive user data
Access control policy	Limits who can access biometric records and system functions
Secure transmission	Protects data moving between terminals, servers, and platforms

9.6 Template Storage and Matching Security

During enrollment, the biometric template is created and stored in the authorized biometric database, terminal, or system architecture, depending on deployment configuration. During authentication, the live biometric sample is processed into a new template or feature vector and compared against stored templates.

Armatura's irreversibility material describes this process as collecting and processing biometric images, extracting relevant biometric features, and comparing them with features stored in the internal template or database to complete authentication. It also states that since complete biometric images are not stored after data collection and feature extraction, the stored feature data cannot be interpreted or reversed to reconstruct the complete biometric images.

This gives clients a practical understanding of how biometric matching can occur without storing raw images as the primary authentication asset.

9.7 Protection of Other Sensitive User Information

Biometric systems often handle additional user information beyond biometric templates. This may include user names, user IDs, profile photos, access levels, department information, time schedules, device permissions, and event logs. These data elements must also be protected because they can reveal personal or operational information.

Armatura's material states that AES-256 encryption is extended to sensitive user information such as usernames, user IDs, and user photos, supporting broader protection of user data during storage and transmission.

For clients, this means biometric data protection should not be treated as a standalone feature. It should be part of a broader secure identity management architecture.

9.8 Recommended Whitepaper Wording for Client Assurance

For the official whitepaper, the following positioning is recommended:

Armatura biometric authentication is designed to protect user privacy through a secure feature-template architecture. During enrollment and authentication, biometric images are processed to extract the necessary mathematical features required for matching. Complete raw biometric images are not stored for routine biometric comparison after feature extraction. The resulting biometric templates are non-interpretable and designed to be irreversible, reducing the risk of reconstructing the original face or palm image. In addition, Armatura applies AES-256 encryption to biometric templates and sensitive user information during storage and transmission, providing a layered security model for enterprise biometric access control.

This language is strong, technical, and client-friendly, while avoiding exaggerated claims.

9.9 Chapter Summary

Armatura's biometric template protection architecture is based on data minimization, feature extraction, template irreversibility, and encryption. The system processes biometric images to extract the features required for authentication, discards unnecessary biometric information, avoids routine storage of raw biometric images, and protects stored templates with AES-256 encryption.

This privacy-oriented architecture helps clients deploy biometric access control with greater confidence, reducing the risk associated with biometric data exposure while preserving the security and convenience benefits of biometric authentication.

10. Performance Evaluation and Test Results

Biometric systems should be evaluated using measurable performance indicators. Recognition accuracy, false acceptance risk, false rejection behavior, threshold configuration, and database scale are all critical considerations in access control deployments.

A biometric system that is too permissive may increase the risk of unauthorized access. A system that is too strict may reject legitimate users and create operational friction. Therefore, performance evaluation must balance security and usability.

Armatura's facial and palm authentication test reports define key metrics including False Acceptance Rate, False Rejection Rate, Equal Error Rate, and True Acceptance Rate.

10.1 Key Performance Metrics

The following metrics should be used consistently throughout the whitepaper.

Metric	Definition	Security Meaning
FAR — False Acceptance Rate	The rate at which the system incorrectly accepts a different person as a match	Lower FAR means lower unauthorized acceptance risk
FRR — False Rejection Rate	The rate at which the system incorrectly rejects the correct person	Lower FRR means better user convenience
EER — Equal Error Rate	The point at which FAR and FRR are equal	Used as a general algorithm performance indicator
TAR — True Acceptance Rate	The rate at which the system correctly accepts legitimate matching attempts	Higher TAR means better legitimate-user recognition

Armatura's facial authentication test report defines FAR as the rate at which feature templates from different samples are incorrectly accepted when the similarity value is greater than or equal to the threshold. It defines FRR as the rate at which feature templates from the same sample are incorrectly rejected when the similarity value is below the threshold. The report defines EER as the point on the FAR/FRR curve where FAR equals FRR, and TAR as the proportion of correctly recognized same-person images.

The palm authentication test report uses the same performance framework, defining FAR, FRR, EER, and TAR for palm authentication evaluation.

10.2 1:1 Verification and 1:N Identification

Biometric performance must be interpreted differently depending on the matching mode.

1:1 verification compares the live biometric sample against a claimed identity. For example, a user may present a card, QR code, mobile credential, or user ID, and the system verifies whether the face or palm matches that claimed identity.

1:N identification compares the live biometric sample against a database of enrolled users. The system searches across many templates and identifies the best match.

Mode	Question Answered	Typical Use Case
1:1 verification	"Is this person the claimed user?"	Card + biometric, ID + biometric, high-security verification
1:N identification	"Who is this person in the enrolled population?"	Walk-up face or palm recognition without presenting a credential

1:N identification is generally more demanding because the system compares against a larger population. As the enrolled population grows, threshold configuration becomes increasingly important.

10.3 Threshold Configuration

A biometric system uses similarity thresholds to determine whether a comparison should be accepted or rejected. When the similarity score meets or exceeds the configured threshold, the system may treat the comparison as a match. When the score falls below the threshold, the system rejects the comparison.

Threshold configuration directly affects FAR and FRR.

A lower threshold may improve convenience by reducing false rejections, but it may increase false acceptance risk. A higher threshold may improve security by reducing false acceptance risk, but it may increase false rejection. Therefore, threshold selection must be aligned with the client's operational risk level.

Threshold Strategy	Effect	Security Meaning
Convenience-oriented	Lower FRR, faster user experience	Low-risk or high-throughput areas
Balanced	Moderate FAR and FRR	General enterprise access
Security-oriented	Lower FAR, stricter acceptance	Data centers, laboratories, restricted zones
Multi-factor	Biometric plus card, PIN, mobile credential, or approval rule	Critical infrastructure and high-risk environments

Armatura's test reports include recommended threshold determination methods for both 1:1 and 1:N scenarios. The facial authentication report describes 1:1 threshold determination using similarity scores and 1:N threshold determination by selecting the score corresponding to zero false acceptance and the highest TAR / lowest false rejection behavior. The palm authentication report uses the same threshold selection principle for 1:N comparison, selecting the score that maintains zero false acceptances while preserving the highest possible TAR and lowest false rejection behavior.

10.4 Facial Authentication Test Results

Armatura's facial authentication test report includes both standard library 1:1 results and a 1,000,000-subject database 1:N test result.

For the **standard library 1:1 facial authentication test**, the report provides the following results:

Facial 1:1 Metric	Result
EER	0.046%
FRR at FAR = 1e-3	0.050%
FRR at FAR = 1e-4	0.130%
FRR at FAR = 1e-5	0.448%
FRR at FAR = 1e-6	0.904%
FRR at FAR = 0	1.630%
TAR at EER	99.954%
TAR at FAR = 1e-3	99.950%
TAR at FAR = 1e-4	99.870%
TAR at FAR = 1e-5	99.552%
TAR at FAR = 1e-6	99.096%
TAR at FAR = 0	98.370%

For the **1,000,000-subject database 1:N facial authentication test**, the report states that at score 24, the system achieved FAR 0.000%, FRR 0.041%, and TAR 99.959%.

Facial 1:N Metric	Result
Database scale	1,000,000 subjects
Score	24
FAR	0.000%
FRR	0.041%
TAR	99.959%

These results should be presented in the final whitepaper as controlled test results under the stated test conditions. For client deployments, performance may vary depending on device model, firmware version,

enrollment quality, environment, database size, threshold configuration, and installation conditions.

10.5 Palm Authentication Test Results

Armatura's palm authentication test report includes both standard library 1:1 results and a 100,000-subject database 1:N result.

For the **standard library 1:1 palm authentication test**, the report provides the following results:

Palm 1:1 Metric	Result
EER	0.1872%
FRR at FAR = 1e-3	0.2506%
FRR at FAR = 1e-4	0.6765%
FRR at FAR = 1e-5	1.1397%
FRR at FAR = 1e-6	1.5921%
FRR at FAR = 0	2.6086%
TAR at EER	99.8128%
TAR at FAR = 1e-3	99.7494%
TAR at FAR = 1e-4	99.3235%
TAR at FAR = 1e-5	98.8603%
TAR at FAR = 1e-6	98.4079%
TAR at FAR = 0	97.3914%

For the **100,000-subject database 1:N palm authentication test**, the report states that at score 47, the system achieved FAR 0.000%, FRR 1.485%, and TAR 98.515%.

Palm 1:N Metric	Result
Database scale	100,000 subjects
Score	47
FAR	0.000%
FRR	1.485%
TAR	98.515%

These palm results demonstrate the feasibility of large-scale contactless palm authentication with zero false acceptances under the reported test condition.

10.6 Interpreting the Results for Clients

For clients, the most important message is not simply that one number is high or low. The key message is that biometric performance must be understood in context.

A high TAR indicates strong recognition of legitimate users. A low FAR indicates stronger protection against unauthorized acceptance. A low FRR indicates smoother daily user experience. EER provides a useful overall measure, but enterprise access control decisions should be based on the required risk level of each access point.

For example:

Area Type	Recommended Security Posture
General office entrance	Balanced threshold, fast user flow
Executive floor	Slightly stricter threshold, possible multi-factor authentication
Data center	Security-oriented threshold, anti-spoofing required
Laboratory	Security-oriented threshold, strong audit trail
Visitor access	Biometric plus visitor workflow and limited access validity
Industrial facility	Threshold adjusted for environmental conditions and user behavior

The final whitepaper should state that Armatura biometric thresholds can be configured according to deployment requirements, balancing security and user convenience.

10.7 Chapter Summary

Armatura evaluates biometric performance using standard recognition metrics including FAR, FRR, EER, and TAR. Facial authentication test results show strong 1:1 performance and a reported 1,000,000-subject 1:N result with FAR 0.000%, FRR 0.041%, and TAR 99.959%. Palm authentication test results show strong 1:1 performance and a reported 100,000-subject 1:N result with FAR 0.000%, FRR 1.485%, and TAR 98.515%.

These results should be communicated as part of a broader biometric assurance model that includes threshold configuration, liveness detection, template protection, deployment conditions, and access control policy.

11. Deployment Architecture and Integration Considerations\

Biometric authentication delivers the greatest value when it is deployed as part of a complete access control ecosystem. A biometric terminal alone cannot define the full security posture of a facility. It must operate together with access controllers, management software, user databases, network infrastructure, encryption mechanisms, audit logs, access policies, and third-party integrations.

Armatura's biometric technology is intended to function as part of a broader access control architecture, combining hardware, software, biometric algorithms, user management, and secure data processing. The uploaded Armatura irreversibility document describes the Armatura Access Control System as a comprehensive solution that includes software, hardware, mobile applications, cloud platforms, and biometric technology.

11.1 Biometric Deployment Model

A typical biometric access control deployment includes several layers:

Layer	Function
Biometric terminal	Captures face or palm input and performs acquisition, preprocessing, liveness, and recognition
Access controller	Enforces door, relay, lock, turnstile, or gate control logic
Management software	Manages users, permissions, devices, schedules, logs, and policies
Biometric database	Stores protected biometric templates and user identity records
Network layer	Connects terminals, controllers, servers, and client workstations
Security layer	Provides encryption, authentication, access control, and auditability
Integration layer	Connects the system with HR, visitor, identity, building, or security platforms

The exact architecture may vary depending on the project. Some deployments may perform matching locally on the terminal. Others may use server-side template management. Some high-security deployments may require multi-factor authentication, centralized policy enforcement, or integration with third-party identity systems.

11.2 Edge, Server, and Hybrid Authentication

Armatura biometric deployments can be discussed in three general architecture models.

Edge authentication

The biometric terminal performs acquisition, feature extraction, liveness detection, and local matching. This model is suitable for fast authentication, reduced dependency on network latency, and distributed access points.

Server-based authentication

The terminal captures biometric input and sends protected data or recognition requests to a centralized server. This model is useful when centralized management, large databases, or unified policy control is required.

Hybrid authentication

The terminal performs time-sensitive functions locally, while the server manages enrollment, synchronization, reporting, templates, access levels, and system-wide administration. This model balances speed, resilience, and centralized control.

Architecture	Advantages	Considerations
Edge	Fast response, local resilience, reduced network dependency	Requires secure terminal management and synchronization
Server-based	Centralized control, easier large-scale policy management	Requires network availability and server capacity planning
Hybrid	Balanced performance and management flexibility	Requires careful design of synchronization and failover behavior

For enterprise access control, hybrid architecture is often the most practical because it allows local authentication speed while preserving centralized management.

11.3 Enrollment Workflow

Enrollment is the process of registering a user's biometric template into the system. A high-quality enrollment process is essential because poor enrollment quality can affect recognition performance throughout the user lifecycle.

A recommended enrollment workflow includes:

1. Create or import the user identity record.
2. Assign user ID, department, access group, role, and validity period.
3. Capture face and/or palm biometric samples.
4. Perform quality assessment and recapture if necessary.
5. Extract biometric features and generate the biometric template.
6. Encrypt and store the template according to system policy.
7. Synchronize the user and template to authorized terminals or servers.
8. Test authentication under expected operating conditions.
9. Activate the user's access permissions.

Armatura's irreversibility material supports this workflow by explaining that biometric images are collected, preprocessed, and converted into extracted features for authentication, while original images are not stored after feature extraction.

11.4 Authentication Workflow at the Access Point

During daily use, the biometric authentication process at the access point should be fast, secure, and policy-driven.

A recommended authentication workflow is:

1. User approaches the biometric terminal.
2. Terminal captures face or palm input.
3. System performs preprocessing and quality assessment.
4. System performs liveness detection and anti-spoofing analysis.
5. System extracts biometric features.
6. System compares live features against enrolled templates.
7. Matching result is evaluated against the configured threshold.
8. Access control policy is checked.
9. Door, turnstile, elevator, or gate action is triggered if permitted.
10. Event log is generated for audit and reporting.

This workflow ensures that recognition is only one part of the decision. The final access result should also depend on permissions, schedules, access groups, door status, anti-passback logic, visitor validity, and other policy conditions.

11.5 Integration with Access Control Hardware

Biometric authentication must interact with the physical access control layer. Depending on the project, this may include:

Hardware Element	Integration Purpose
Door lock	Unlocks after successful authentication and policy approval
Turnstile or flap barrier	Controls pedestrian flow
Speed gate	Supports high-throughput entry with biometric verification
Elevator control	Restricts floor access based on user permissions
Alarm input	Receives door forced-open, door held-open, tamper, or emergency signals
Exit button	Supports safe egress
Door contact	Confirms door position
Access controller	Enforces relay logic and access policy

In high-security environments, biometric terminals should not be treated as standalone door-opening devices only. They should be integrated with access controllers and management software to ensure policy consistency, auditability, and secure door control.

11.6 Integration with Enterprise Systems

Biometric access control often needs to connect with other enterprise platforms. These integrations reduce manual administration and help synchronize identity data across the organization.

Common integration targets include:

System	Integration Value
HR system	Automatically synchronize employee records and employment status
Visitor management system	Support temporary access and visitor identity workflow
Identity and access management platform	Align physical identity with enterprise identity governance
Video surveillance system	Link access events with video evidence
Building management system	Coordinate access events with building operations
Time attendance system	Use biometric authentication for attendance records
Security operations platform	Centralize monitoring, alerts, and incident response

For the final whitepaper, Armatura can position its biometric technology as integration-ready, especially for projects where access control, time attendance, visitor management, and identity lifecycle management are connected.

11.7 Network and Data Security Considerations

Biometric deployment must be supported by strong network security. Since biometric templates and user records are sensitive, data must be protected during storage, synchronization, and transmission.

Armatura's template protection document states that AES-256 encryption is used to protect biometric templates and sensitive user information during storage and transmission.

Recommended deployment security considerations include:

Area	Recommendation
Network segmentation	Separate access control devices from general office networks where possible
Encrypted transmission	Protect communication between terminals, servers, and management software
Strong administrator accounts	Use role-based permissions and secure administrator authentication
Device hardening	Disable unused services and protect terminal configuration
Template protection	Store only protected templates, not raw biometric images
Event logging	Record authentication, enrolment, configuration, and administrator actions
Backup and recovery	Protect system configuration and user data with secure backup policies
Firmware management	Maintain controlled update and patching procedures

The goal is to secure the complete biometric ecosystem, not only the recognition algorithm.

11.8 Scalability and Database Planning

Large-scale biometric deployments require careful planning around database size, recognition mode, synchronization, and performance.

1:N identification against a large population requires more computational resources than 1:1 verification. For very large databases or high-throughput entrances, the system architecture should be designed around expected transaction volume, number of enrolled users, peak authentication rate, number of terminals, and network performance.

Key planning questions include:

Planning Question	Reason
How many users will be enrolled?	Determines database and matching requirements
Which authentication mode will be used?	1:1 and 1:N have different performance profiles
How many access points are required?	Determines terminal and controller distribution
What is the peak authentication volume?	Impacts throughput and latency design
Is offline authentication required?	Determines local template storage and synchronization strategy
Are multiple sites involved?	Requires centralized management and replication strategy
What is the risk level of each access point?	Determines thresholds and multi-factor requirements

Armatura's reported facial authentication test includes a 1,000,000-subject database 1:N result, while the palm authentication test includes a 100,000-subject database 1:N result. These test results can help clients understand the scalability potential of the biometric technologies, while actual project design should still account for deployment-specific conditions.

11.9 Recommended Deployment Scenarios

Armatura biometric access control can be applied across different security levels.

Planning Question	Reason
How many users will be enrolled?	Determines database and matching requirements
Which authentication mode will be used?	1:1 and 1:N have different performance profiles
How many access points are required?	Determines terminal and controller distribution
What is the peak authentication volume?	Impacts throughput and latency design
Is offline authentication required?	Determines local template storage and synchronization strategy
Are multiple sites involved?	Requires centralized management and replication strategy
What is the risk level of each access point?	Determines thresholds and multi-factor requirements

Different access points may require different authentication policies. A lobby entrance may prioritize throughput, while a data center may prioritize the lowest possible false acceptance risk.

11.10 Operational Best Practices

A successful biometric deployment depends not only on technology, but also on operational discipline.

Recommended best practices include:

Best Practice	Purpose
Conduct site survey	Confirm lighting, mounting height, user flow, and environmental conditions
Define security levels	Match authentication policy to the risk level of each area
Use high-quality enrollment	Improve recognition stability and reduce false rejection
Train administrators	Ensure correct user management and threshold configuration
Provide user guidance	Help users understand proper face or palm presentation
Monitor event logs	Detect abnormal access patterns or repeated failures
Review threshold settings	Balance security and convenience after real-world operation
Establish fallback methods	Support users who cannot authenticate biometrically
Protect privacy notices	Communicate biometric processing policy to users where required
Maintain update procedures	Keep terminals and management systems controlled and current

For high-security clients, it is also recommended to combine biometric authentication with access levels, schedules, anti-passback, video verification, or multi-factor authentication.

11.11 Integration Considerations for Consultants and System Integrators

Consultants and system integrators evaluating Armatura biometric solutions should consider the following design factors:

Design Area	Key Consideration
Authentication mode	1:1 verification, 1:N identification, or multi-factor
Biometric modality	Face, palm, fingerprint, or combination
Anti-spoofing requirement	Required for high-security and unsupervised access points
Database size	Number of enrolled users and expected growth
Throughput	Expected users per minute at peak time
Network topology	Local, centralized, cloud-connected, or hybrid
Failover	Offline authentication and recovery behavior
Privacy requirements	Consent, notices, retention, and access control to biometric data
Integration API	HR, visitor, time attendance, video, or security platform integration
Maintenance model	Firmware updates, template synchronization, backups, and support

These factors should be defined early in the project to ensure the biometric system is designed correctly from the start.

11.12 Chapter Summary

Armatura biometric technology should be deployed as part of a complete access control architecture that includes terminals, controllers, software, protected biometric databases, encrypted communication, access policies, audit logs, and enterprise integrations.

A successful deployment requires careful planning around enrollment quality, authentication workflow, liveness detection, threshold configuration, database scale, network security, system integration, and operational governance. By combining biometric intelligence with secure access control architecture, Armatura enables clients to deploy identity-driven physical security systems that are contactless, scalable, and enterprise-ready.

12. Compliance, Privacy, and Responsible Biometric Use

Biometric authentication provides strong identity assurance, but it also requires a disciplined approach to privacy, governance, security, and responsible deployment. Unlike traditional credentials, biometric characteristics are intrinsically linked to the individual. A card can be replaced, a password can be reset, and a PIN can be changed, but a person's face, palm, or fingerprint cannot be changed in the same way. For this reason, biometric systems must be designed and deployed with appropriate technical, organizational, and policy safeguards.

Armatura's biometric architecture is designed around a privacy-conscious model that reduces exposure of raw biometric data. The system processes face and palm images to extract the necessary biometric features for authentication, while the uploaded Armatura template protection material states that original facial or palm images are not stored after feature extraction and that only required biometric features are retained for authentication.

12.1 Biometric Data as Sensitive Identity Data

Biometric data used for uniquely identifying a natural person is treated as a sensitive category of personal data in many regulatory frameworks. Under GDPR Article 9, biometric data processed for the purpose of uniquely identifying a person is listed as a special category of personal data. (GDPR)

This means that biometric access control deployments should not be treated as ordinary IT installations. They should be implemented with clear purpose limitation, documented processing practices, appropriate legal basis, user transparency, access controls, data retention policies, and strong information security measures.

For Armatura clients, this whitepaper should position biometric technology as a high-assurance identity tool that must be paired with responsible governance. The technology provides the security foundation, while the client's operating policies, user notices, retention rules, administrator controls, and compliance program complete the governance model.

12.2 Privacy-by-Design Architecture

Privacy by design means that privacy and data protection principles are embedded into the technology and operational workflow from the beginning. GDPR Article 25 requires appropriate technical and organizational measures so that, by default, only personal data necessary for each specific purpose is processed. (GDPR)

Armatura's biometric architecture supports this concept through a feature-template model. The system does not need to retain the full biometric image for routine authentication. Instead, it extracts required biometric features and converts them into mathematical templates used for matching. Armatura's uploaded material states that only a small portion of the original biometric information required for authentication is retained, while unnecessary information is discarded and not stored; the resulting templates are described as non-interpretable and not usable to reverse-engineer complete biometric images.

In client-facing terms, this supports a privacy-by-design message:

Privacy Principle	Armatura-Oriented Implementation
Purpose limitation	Biometric data is processed for identity authentication and access control
Data minimization	Only the biometric features required for matching are retained
Storage limitation	Complete raw biometric images are not stored for routine authentication after feature extraction
Template irreversibility	Templates are designed as non-interpretable mathematical representations
Encryption	Biometric templates and sensitive user information are encrypted
Access control	System administration should be limited to authorized roles
Auditability	Enrollment, authentication, and administrative actions should be logged

12.3 Security of Processing

Security of biometric data requires both technical and organizational controls. GDPR Article 32 requires controllers and processors to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including encryption, confidentiality, integrity, availability, resilience, restoration capability, and regular testing of security measures. (GDPR)

Armatura's biometric template protection material states that AES-256 encryption is applied to biometric templates for secure storage and transmission, and that encryption is also extended to sensitive user information such as usernames, user IDs, and user photos.

For enterprise deployments, encryption should be part of a layered security model that also includes:

Security Control	Purpose
Encrypted template storage	Protect biometric templates if storage is accessed without authorization
Encrypted data transmission	Protect biometric and user data moving between terminals, servers, and platforms
Role-based administration	Restrict access to biometric enrollment, deletion, export, and configuration functions
Audit logs	Record authentication events, enrollment changes, administrator activity, and exceptions
Network segmentation	Reduce exposure of access control devices to general network traffic
Backup and recovery	Protect system continuity and recoverability
Patch and firmware management	Maintain controlled system updates
Incident response process	Define response procedures for suspected data or system compromise

12.4 Presentation Attack Detection and Standards Alignment

Responsible biometric deployment also requires protection against spoofing and presentation attacks. Presentation attack detection, often called PAD or anti-spoofing, is the process of detecting whether a presented biometric sample is genuine or an attack instrument. ISO/IEC 30107-1:2023 establishes terms and definitions for specifying, characterizing, and evaluating biometric presentation attack detection methods, but it does not standardize specific detection algorithms, sensors, or countermeasures. (ISO)

Armatura's face and palm biometric architectures include liveness detection before recognition. The face anti-spoofing material describes visible-light and near-infrared analysis, liveness score prediction, and fusion-based decision-making before proceeding to face recognition. The palm material describes liveness detection using reflection patterns, material texture, light distribution, surface structure, and infrared palm vein characteristics.

For the final published whitepaper, Armatura should avoid stating that ISO/IEC 30107-1 certifies a specific algorithm unless there is a separate test report or certification. A stronger and safer wording is:

Armatura's biometric architecture is designed with presentation attack detection principles in mind, including liveness detection, multimodal sensing, and feature-level analysis. These mechanisms support the broader security objectives described in PAD-related standards such as ISO/IEC 30107, while final project compliance and certification depend on the applicable product configuration, test scope, and deployment requirements.

12.5 Transparency and User Communication

A responsible biometric deployment should clearly inform users about how biometric data is processed. Users should understand what biometric modality is used, why it is used, what data is collected, whether raw images are stored, how templates are protected, who can access the system, how long data is retained, and how users can exercise applicable rights.

Recommended user communication topics include:

Topic	Recommended Content
Purpose	Biometric authentication for access control, time attendance, visitor management, or identity verification
Modality	Face, palm, fingerprint, or multimodal authentication
Data processing	Images are processed to extract features for matching
Template protection	Templates are encrypted and designed to be non-interpretable
Retention	Templates are retained only while required for the defined purpose
User rights	Access, correction, deletion, restriction, or other rights depending on local law
Contact point	Internal privacy, HR, security, or data protection contact

Armatura's uploaded irreversibility material references GDPR-aligned user rights such as access, rectification, deletion, and restriction of processing.

12.6 Data Retention and Deletion

Biometric data should not be retained indefinitely without a valid operational purpose. In access control environments, retention is commonly linked to the user's employment status, visitor validity period, contractor authorization, or membership in an access-controlled population.

Recommended retention principles include:

Data Type	Recommended Retention Principle
Biometric template	Retain only while the user is authorized to use biometric access
Enrollment record	Retain according to HR, security, or access control policy
Access event log	Retain according to audit, security, and legal requirements
Visitor biometric record	Retain only for the approved visitor validity period, unless legally required otherwise
Deleted user record	Remove or anonymize according to policy and legal requirements

For high-security projects, retention rules should be documented before deployment, approved by the client's security and legal teams, and enforced through the management platform.

12.7 Responsible Use Principles

Armatura's biometric whitepaper should include a responsible use statement. This helps reassure clients that Armatura views biometrics as an identity assurance technology requiring careful governance.

Recommended responsible use principles:

Principle	Meaning
Lawful and defined purpose	Biometrics should be deployed for a clear access control or identity verification purpose
Proportionality	The biometric modality and authentication policy should match the risk level of the site
Transparency	Users should be informed about biometric processing
Security by design	Templates, communications, and administrative access should be protected
Non-discrimination	Deployment should consider usability across diverse user populations
Human oversight	Exceptions, enrollment issues, and access disputes should have defined procedures
Fallback options	Alternative authentication should be available where appropriate
Regular review	Thresholds, logs, and policies should be periodically reviewed

12.8 Chapter Summary

Armatura biometric technology is designed to support privacy-conscious and security-oriented deployment through template irreversibility, data minimization, encryption, liveness detection, and secure system architecture. However, responsible biometric use also requires client-side governance, including user notice, legal basis, retention rules, access control, administrator authorization, audit logging, and regular review.

By combining Armatura's technical protections with appropriate organizational policies, clients can deploy biometric access control as a trusted, secure, and privacy-aware identity layer.

13. Enterprise and High-Security Use Cases

Armatura biometric technology is designed for environments where organizations require secure, contactless, scalable, and user-friendly identity authentication. The combination of deep learning face recognition, bi-modal palm authentication, liveness detection, template irreversibility, and encrypted template protection makes the technology suitable for a broad range of enterprise and high-security applications.

The purpose of this section is to translate Armatura's biometric capabilities into practical deployment scenarios for clients, consultants, and system integrators.

13.1 Corporate Headquarters and Smart Offices

Corporate headquarters require a balance between security, user experience, and operational efficiency. Employees need to move quickly through entrances, turnstiles, elevator lobbies, and restricted office zones, while security teams need reliable access logs and protection against credential sharing.

Armatura face recognition can support fast contactless entry, while bi-modal palm authentication can provide an additional option for users or higher-security internal areas. Palm authentication is especially suitable where contactless hygiene and user convenience are important, because Armatura's palm material identifies contactless authentication and convenient palm positioning as key advantages of its bi-modal palm approach.

Recommended configuration:

Area	Recommended Authentication
Main lobby	Face or palm recognition
Turnstile entrance	Face recognition for high throughput
Elevator lobby	Face or palm linked to floor permissions
Executive floor	Biometric plus stricter threshold
Records room	Palm or face + card
Security office	Multi-factor biometric authentication

13.2 Data Centers and Critical Infrastructure

Data centers, utility facilities, telecom sites, energy plants, logistics hubs, and other critical infrastructure environments require stronger identity assurance than ordinary office entrances. Unauthorized access can create operational, financial, and security risks.

For these sites, Armatura's bi-modal palm authentication is well suited because it combines visible-light palm recognition with infrared palm vein recognition. Palm vein authentication captures internal vein patterns beneath the skin, and the uploaded palm material states that these patterns are not visible to the naked eye and are difficult to observe or replicate.

Recommended configuration:

Security Layer	Recommended Practice
Perimeter entrance	Face or palm recognition with anti-spoofing
Mantrap or secure vestibule	Palm + card or face + palm
Server room	Strict threshold and multi-factor authentication
Network operations area	Biometric access with detailed audit logs
Contractor access	Temporary credential plus biometric verification
Emergency access	Defined override process with event logging

13.3 Laboratories, Research Facilities, and Clean Environments

Laboratories and research facilities often require both hygiene and security. Users may wear gloves, masks, or protective equipment. Access may need to be restricted by role, project, certification, or time schedule.

Palm authentication provides a contactless alternative to fingerprint readers or shared touch devices. Face recognition can support general access, while palm recognition can be used for higher-security rooms or where face presentation may be affected by masks or protective gear.

Recommended configuration:

Environment	Recommended Authentication
General lab entrance	Face or palm
Cleanroom entrance	Contactless palm
Restricted R&D room	Face + palm or palm + card
Chemical storage	Biometric plus supervisor-defined access group
Equipment room	Palm authentication with event log review

13.4 Healthcare Facilities

Hospitals, clinics, laboratories, pharmacies, and healthcare campuses require reliable identity authentication while minimizing touchpoints. Healthcare environments also require careful access control to medication storage, patient records areas, laboratories, operating rooms, staff-only zones, and equipment rooms.

Contactless face and palm authentication can reduce reliance on shared touch devices. Palm authentication is especially suitable for hygiene-sensitive areas, provided that deployment policies address user consent, local privacy requirements, and fallback authentication.

Recommended configuration:

Area	Recommended Authentication
Staff entrance	Face or palm
Pharmacy storage	Palm + card or face + PIN
Laboratory	Contactless palm
Medical records room	Biometric plus role-based access
Operating department	Palm or multi-factor authentication
Visitor-managed area	Visitor credential with limited access validity

13.5 Airports, Transport Hubs, and High-Throughput Facilities

Airports, rail stations, metro systems, logistics terminals, and other transport hubs often require high-throughput authentication for staff, contractors, and restricted operational areas. These environments require fast recognition, strong auditability, and reliable access control across distributed doors and gates.

Face recognition is suitable for high-throughput staff entry because users can authenticate naturally while moving through controlled access points. Palm authentication can be deployed for restricted operational areas, staff-only zones, maintenance facilities, or high-assurance access points.

Recommended configuration:

Area	Recommended Authentication
Staff entrance	Face recognition
Airside access	Face + card or palm + card
Baggage handling zone	Biometric with role-based access
Control room	Multi-factor biometric authentication
Contractor entrance	Temporary credential plus biometric verification
Maintenance area	Palm or face with schedule-based access

13.6 Industrial and Manufacturing Sites

Industrial environments introduce unique challenges. Workers may carry tools, wear protective gear, work in shifts, or operate in areas where cards are easily lost or damaged. Traditional credentials may be inconvenient or unreliable.

Palm authentication can provide a practical contactless option, while face recognition can support general entry where lighting and camera placement are controlled. For outdoor or semi-outdoor environments, site survey and device selection are especially important.

Recommended configuration:

Area	Recommended Authentication
Factory entrance	Face or palm
Production line access	Palm authentication
Tool room	Biometric plus access group
Warehouse	Face or palm linked to shift schedule
Hazardous area	Palm + card or biometric + supervisor policy
Contractor access	Limited-time biometric or credential-based access

13.7 Education and Campus Security

Universities, schools, and campuses require scalable identity management for students, faculty, staff, contractors, and visitors. Security must be balanced with user convenience and privacy.

Biometric access control may be applied selectively to sensitive areas rather than universally. Examples include laboratories, dormitory entrances, data centers, libraries, faculty-only zones, and examination areas.

Recommended configuration:

Area	Recommended Authentication
Staff-only entrance	Face or palm
Research laboratory	Palm authentication
Data room	Multi-factor biometric authentication
Dormitory entrance	Face or palm, subject to local policy
Library restricted area	Biometric or card + biometric
Visitor access	Visitor workflow with temporary validity

13.8 Financial Institutions and Secure Offices

Banks, financial service providers, trading offices, and payment infrastructure operators require strong access control, auditability, and risk management. Biometric authentication can reduce credential sharing and strengthen accountability.

Recommended configuration:

Area	Recommended Authentication
Main staff entrance	Face recognition
Cash handling area	Palm + card
Vault support area	Multi-factor biometric authentication
Trading floor	Face or palm with audit logging
Executive area	Palm or face + policy-based access
Records/archive room	Biometric access with event review

13.9 Visitor Management and Temporary Access

Visitor workflows often require a different security model from employee access. Visitors may be authorized for a limited time, a limited area, or a specific host. Biometrics can be used where legally permitted and operationally appropriate, but many deployments may combine visitor ID verification, QR code, RFID card, or escorted access.

Recommended visitor model:

Step	Recommended Workflow
Pre-registration	Host submits visitor details and visit purpose
Check-in	Visitor identity is verified at reception
Credential issuance	Temporary QR code, card, or biometric enrolment where permitted
Access restriction	Visitor access limited by time, area, and host
Check-out	Credential expires or is revoked
Log review	Access events retained according to policy

13.10 Recommended Use Case Matrix

Use Case	Face Recognition	Bi-Modal Palm	Multi-Factor	Key Benefit
Office lobby	High	Medium	Optional	Fast contactless access
Turnstile entrance	High	Medium	Optional	High throughput
Data center	Medium	High	Recommended	Strong assurance
Laboratory	Medium	High	Optional / Recommended	Contactless secure access
Healthcare	Medium	High	Optional	Hygiene and controlled access
Factory	Medium	High	Optional	Practical credential-free access
Airport staff area	High	Medium/High	Recommended for airside	Throughput and auditability
Visitor access	Medium	Optional	Optional	Temporary controlled identity
Executive area	Medium / High	High	Recommended	Restricted access
Critical infrastructure	Medium	High	Recommended	High-security assurance

13.11 Chapter Summary

Armatura biometric technology can support a wide range of enterprise and high-security use cases, from corporate offices and smart buildings to data centers, laboratories, healthcare facilities, industrial sites, transportation hubs, and critical infrastructure.

Face recognition provides fast and natural contactless access. Bi-modal palm authentication provides strong identity assurance through the combination of visible palm characteristics and internal palm vein recognition. Liveness detection, encrypted templates, and access control integration strengthen the overall security architecture.

14. Conclusion

Modern access control is moving beyond cards, PINs, passwords, and mechanical credentials toward identity-driven security. Organizations need to know not only that a credential is valid, but that the person using it is the authorized individual. Biometric authentication addresses this requirement by linking access decisions to physical identity.

Armatura's biometric technology is designed to support this transition through a secure, contactless, privacy-conscious, and scalable authentication architecture. The system combines deep learning-based face recognition, bi-modal palm authentication, liveness detection, template irreversibility, encryption, and access control integration.

The deep learning face recognition architecture enables fast and intuitive authentication by detecting the face, assessing liveness, aligning the facial image, extracting high-dimensional features, generating embeddings, and comparing them with enrolled templates. Face recognition is particularly suitable for high-throughput environments such as corporate entrances, turnstiles, smart buildings, transport hubs, and staff access points.

Armatura's bi-modal palm authentication strengthens biometric assurance by combining visible-light palm recognition with infrared palm vein recognition. Visible-light recognition analyzes external palm features such as shape, texture, curvature, and finger position, while infrared palm vein recognition captures internal vein patterns beneath the skin surface. Armatura's own material states that bi-modal palm authentication captures both visible-light and infrared palm images and uses cross-modal fusion to produce a more comprehensive and accurate analysis.

Security against spoofing is central to Armatura's biometric architecture. Facial liveness detection uses visible-light and near-infrared inputs, liveness scoring, feature analysis, and fusion-based decision-making. Palm liveness detection analyzes visible and infrared palm characteristics, including reflection patterns, material textures, light distribution, surface structure, and palm vein properties. These mechanisms support the broader objective of presentation attack resistance in biometric access control.

Privacy and data protection are equally important. Armatura's template protection material states that after biometric images are collected and preprocessed, only the necessary biometric features are extracted and retained, while unnecessary biometric information is discarded and complete biometric images are not stored for routine authentication. It also states that AES-256 encryption is applied to biometric templates and other sensitive user information.

For enterprise clients, the value of Armatura biometrics is not limited to recognition accuracy. The value lies in the complete trust architecture:

Trust Requirement	Armatura-Oriented Capability
Identity assurance	Face, palm, and multimodal biometric authentication
Spoofing resistance	Face and palm liveness detection
Privacy protection	Template irreversibility and data minimization
Secure storage and transmission	AES-256 encryption of templates and sensitive user data
Deployment flexibility	Edge, server, and hybrid access control architectures
Enterprise integration	Compatibility with access control, visitor, HR, and security workflows
Scalability	Support for large user populations and configurable matching policies
User experience	Fast, contactless, and intuitive authentication

The future of access control will be defined by systems that are intelligent, secure, privacy-aware, and frictionless. Armatura's multimodal biometric architecture provides a foundation for this future by transforming biometric authentication into a protected identity assurance layer for modern physical security.

15. Appendix: Metrics, Glossary, Standards, and References

15.1 Biometric Performance Metrics

Term	Full Name	Definition
FAR	False Acceptance Rate	The rate at which the system incorrectly accepts a non-matching user
FRR	False Rejection Rate	The rate at which the system incorrectly rejects a legitimate matching user
EER	Equal Error Rate	The point where FAR and FRR are equal
TAR	True Acceptance Rate	The rate at which the system correctly accepts legitimate matching attempts
FMR	False Match Rate	The proportion of impostor comparisons at or above a
		matching threshold
FNMR	False Non-Match Rate	The proportion of genuine/mated comparisons below a threshold
FPIR	False Positive Identification Rate	The rate at which an identification system returns an incorrect identity
FNIR	False Negative Identification Rate	The rate at which an identification system fails to identify an enrolled person

Armatura's facial authentication report defines FAR, FRR, EER, and TAR and includes formulas and FAR/FRR curve explanation for biometric performance evaluation. NIST's FRTE 1:1 page describes FNMR as the proportion of mated comparisons below a threshold set to achieve a specified FMR, and FMR as the proportion of impostor comparisons at or above that threshold. (NIST Pages)

15.2 Matching Modes

Mode	Description	Typical Use
1:1 Verification	Compares a biometric sample against a claimed identity	Card + biometric, QR + biometric, ID + biometric
1:N Identification	Searches a biometric sample against an enrolled population	Walk-up face or palm access without presenting another credential
Multi-Factor Authentication	Combines biometric authentication with another credential	High-security access points
Multimodal Authentication	Uses more than one biometric modality or sensor channel	Face + palm, visible palm + infrared palm vein

15.3 Biometric Modality Glossary

Term	Definition
Face Recognition	Biometric recognition based on facial features
Palm Recognition	Biometric recognition based on palm shape, texture, palmprint, or palm vein patterns
Palm Vein Recognition	Recognition based on internal vein patterns beneath the palm surface
Visible-Light Palm Recognition	Palm recognition using visible-light imaging of external palm features
Infrared Palm Recognition	Palm recognition using infrared imaging, often used for palm vein analysis
Fingerprint Recognition	Biometric recognition based on fingerprint ridge patterns
Face Embedding	Mathematical representation of facial features used for matching
Palm Code	Mathematical or numerical representation of palm features used for matching
Template	Stored mathematical representation of biometric features
Feature Extraction	Process of converting biometric samples into useful mathematical features
ROI	Region of Interest; the selected image area used for focused biometric processing

15.4 Security and Privacy Glossary

Term	Definition
Liveness Detection	Process of determining whether a biometric sample comes from a genuine live person
Anti-Spoofing	Techniques used to detect and reject fake biometric presentations
Presentation Attack	Attempt to deceive a biometric system using a fake or manipulated biometric sample
PAD	Presentation Attack Detection
Template Irreversibility	Design property that prevents reconstruction of the original biometric image from the template
Data Minimization	Collecting and retaining only the data necessary for the defined purpose
AES-256	Symmetric encryption algorithm using a 256-bit key
Privacy by Design	Embedding privacy protections into technology and processes by default
Access Control Policy	Rules determining who may access which doors, areas, systems, or resources
Audit Log	Record of authentication, administrative, and system events

15.5 Standards and Regulatory References

Reference	Relevance
GDPR Article 9	Treats biometric data used for uniquely identifying a person as special category data
GDPR Article 25	Data protection by design and by default
GDPR Article 32	Security of processing, including encryption and confidentiality measures
ISO/IEC 30107-1:2023	Terms and definitions for biometric presentation attack detection
NIST FRTE / FRVT	Independent evaluation framework for face recognition technology performance

GDPR Article 25 emphasizes data protection by design and default, including processing only personal data necessary for each specific purpose. (GDPR) GDPR Article 32 requires appropriate technical and organizational measures, including encryption and confidentiality, integrity, availability, and resilience of processing systems and services. (GDPR) ISO/IEC 30107-1:2023 establishes PAD-related terms and definitions but does not standardize specific PAD algorithms or sensors. (ISO)

15.6 Recommended Abbreviations

Abbreviation	Meaning
AI	Artificial Intelligence
AES	Advanced Encryption Standard
CNN	Convolutional Neural Network
EER	Equal Error Rate
FAR	False Acceptance Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Rejection Rate
GDPR	General Data Protection Regulation
IR	Infrared
NIR	Near-Infrared
PAD	Presentation Attack Detection
ROI	Region of Interest
TAR	True Acceptance Rate

15.7 Bibliography

Source Category	Recommended Inclusion
Armatura internal technical material	Face recognition, face anti-spoofing, palm recognition, palm anti-spoofing, template irreversibility
Armatura test reports	Facial Authentication Test and Palm Authentication Test
Standards	ISO/IEC 30107 series for PAD terminology and evaluation context
Regulatory references	GDPR Articles 9, 25, and 32
Benchmark references	NIST FRTE/FRVT performance terminology and benchmark context

15.8 Whitepaper Disclaimer

This whitepaper is provided for technical and informational purposes only. Product functions, performance, deployment architecture, and compliance outcomes may vary depending on product model, software version, configuration, database size, environment, installation quality, system integration, and applicable local laws. Biometric system deployment should be assessed by the customer's security, legal, privacy, and compliance teams before implementation. References to regulations or standards are provided for general technical context and do not constitute legal advice or certification.

15.9 Closing Statement

Armatura biometric technology is designed to deliver secure, contactless, intelligent, and privacy-conscious authentication for modern access control. By combining deep learning face recognition, bi-modal palm authentication, liveness detection, irreversible template architecture, encryption, and enterprise deployment flexibility, Armatura provides a trusted biometric foundation for organizations seeking to strengthen physical security while improving user experience.

Address:190 Bluegrass Valley Parkway, Alpharetta, GA 30005
Phone: + 1 (470) 816-1970
Email: sales@armatura.us
Website: www.armatura.us