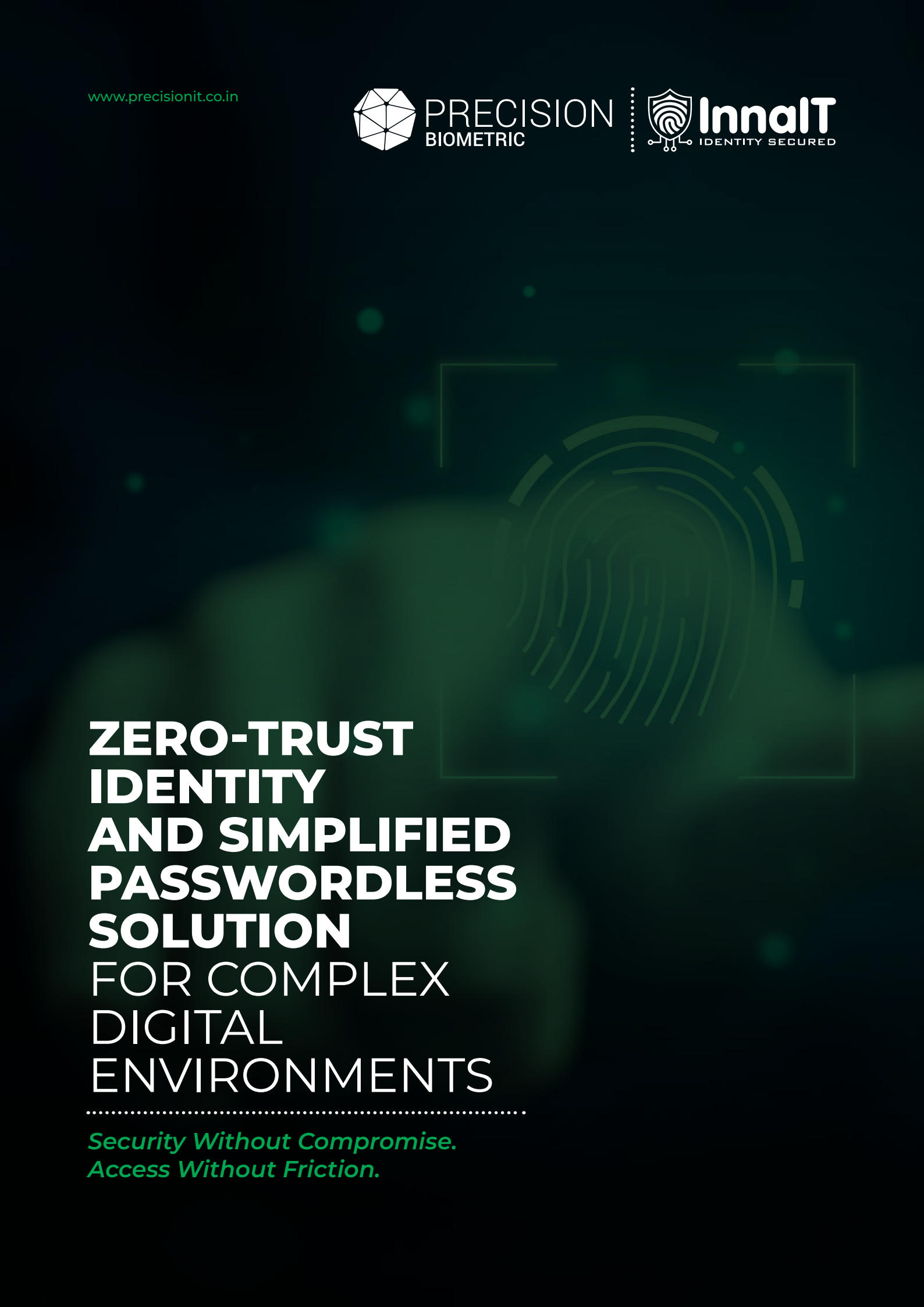
www.precisionit.co.in

PRECISION BIOMETRIC | InnaIT IDENTITY SECURED



ZERO-TRUST IDENTITY AND SIMPLIFIED PASSWORDLESS SOLUTION FOR COMPLEX DIGITAL ENVIRONMENTS

Security Without Compromise.
Access Without Friction.

Enterprise challenges in an evolving digital world

As enterprises accelerate digital transformation, managing identities securely has become more complex. Organizations now operate across cloud, SaaS, on-premises, hybrid, and edge environments. Each environment introduces new identity and access challenges.

The growth of remote and distributed workforces has further expanded the identity attack surface.

Enterprise data is also growing at an unprecedented rate. It is distributed across multiple systems, platforms, and data silos, making it increasingly difficult to control who or what can access sensitive information.

As a result, organizations require continuous identity verification and adaptive access controls that can respond to evolving risks in real-time.

However, many organizations still rely on legacy authentication methods. These approaches often create friction for users while failing to protect against modern identity-based attacks.

Passwords, traditional Single Sign-On (SSO), and conventional Multi-Factor Authentication (MFA) are no longer enough to stop today's sophisticated cyber threats.

Organizations need a modern identity strategy built on Zero Trust and Passwordless authentication. Such an approach continuously verifies every human and non-human identity, secures access to applications and data, reduces cyber risk, and delivers a seamless user experience.

The Business Problem

Rising Identity Risks

62%

of security breaches involve the human element, including compromised credentials, phishing, and social engineering.[1]

Compromised or valid credentials account for

30%

of initial access vectors in APAC, making them the region's second leading cause of cyberattacks.[2]

[1] *2026 Verizon DBIR* | [2] *X-Force Threat Intelligence Index 2026*

Limitations of Traditional Security

SSO:
A compromised account can expose multiple applications

MFA:
Susceptible to phishing, SIM swap, push fatigue, and OTP attacks

Passkeys:
Strong security but challenging to deploy and manage at enterprise scale

Enterprise Identity Challenges

Identity Sprawl: 100+ SaaS applications create fragmented identities

MFA Bypass: Sophisticated attacks continue to evade traditional MFA

Multi-Cloud Complexity: Identities must be secured across hybrid and multi-cloud environments

Poor User Experience: Password resets reduce productivity and increase IT workload

Growing Regulatory & Compliance Requirements: Organizations must comply with evolving global data privacy and security regulations, including PII protection, GDPR, APPI (Japan), and DPDPA (India), driving the need for robust identity and data protection solutions.

Why Passkeys Are Not Enough

Authentication is an event. Trust must be continuous.

Passkeys represent a significant advancement over passwords by providing phishing-resistant, Passwordless authentication. However, authentication is only the beginning of the security journey.

Today's attackers increasingly target what happens after a user successfully logs in. Instead of stealing passwords, they focus on compromising authenticated sessions, browsers, trusted devices, and fallback authentication mechanisms. AI-powered phishing, session hijacking, browser compromise, and malware can still enable unauthorized access without breaking the passkey itself.

A secure enterprise identity strategy must go beyond login. It should continuously verify every user, device, and session throughout the access lifecycle, ensuring trust is maintained even after authentication is complete.

The Need of the Hour

- True end-to-end Passwordless authentication
- Phishing-resistant identity security
- Seamless user experience across devices
- Zero Trust access for every user and application
- Unified identity management across cloud, SaaS, and on-premises environments
- Simplified administration with stronger security

Why InnaIT?

Secure Every Identity. Simplify Every Login.

InnaIT is an identity and authentication platform that uniquely combines Public Key Infrastructure (PKI) and biometrics to deliver a comprehensive solution for modern identity, security, and authentication needs. Designed to support today's digital enterprises, InnaIT enables secure Identity and Access Management (IAM), Zero Trust security frameworks, and Passwordless identity authentication, ensuring seamless yet robust user verification. The platform also provides trusted transaction authorization and digital signing capabilities, safeguarding every interaction with strong cryptographic security and biometric assurance. By integrating these technologies into a single, unified platform, InnaIT empowers organizations to enhance security, simplify the user experience, and build trusted digital ecosystems. Together, they provide:

- **Secure, Passwordless authentication**
- **Trusted digital signing**
- **Robust identity governance**
- **Compliance-ready security infrastructure**

- **CERT-In Certified**
- **FIDO2 & WebAuthn Compatible**
- **PKI - Based Security**
- **Compliance Ready**
- **Secure Encryption**
- **Trusted Digital Identity**

InnaIT Framework

Integrating Solution, Architecture, and Value

InnaIT Framework is a modular identity and authentication platform that brings together biometric hardware, software, and secure authentication services into a single, scalable solution. The framework includes one Server Component and a choice of two Client Components, either a Soft Token or the InnaITKey hardware security key, allowing organizations to deploy the authentication method that best fits their security and operational requirements. It simplifies implementation by eliminating the need to integrate multiple security tools, enabling seamless authentication across applications, and growing with your organization's needs. With centralized, tamper-resistant audit trails and flexible integration through SDKs, InnaIT delivers stronger security, simplified management, and a consistent user experience.

Three-Layer Security Architecture

1. Software Layer – Intelligent Identity Platform

Provides seamless integration and secure access across all enterprise systems. Manage identities and authenticate users securely. Seamlessly integrates enterprise applications to deliver secure access, centralized identity management, and frictionless user authentication.

Key Capabilities:

- Passwordless Authentication
- SSO & MFA
- Identity Provider (IdP)
- Biometric authentication
- APIs, SDKs & enterprise integrations

Business Benefits:

- Seamless user experience
- Rapid Rollouts
- Accelerated Value Realizations
- Reduced password costs
- High user adoption

2. Hardware Layer – InnaITKey Biometric Security Key

A secure, tamper-resistant biometric security key that enables true passwordless authentication. Protects user identities with fingerprint verification, secure encryption, and phishing-resistant access.

Key Capabilities:

- Fingerprint authentication
- Hardware root of trust
- Secure key storage
- USB / NFC connectivity

Business Benefits:

- Phishing-resistant access
- Zero credential exposure
- Strong hardware encryption
- Enhanced user trust

3. Server Layer – Enterprise Identity Services

A centralized authentication server that simplifies enterprise identity management by securely managing users, authentication policies, access controls, and compliance from a single platform.

Key Capabilities:

- Authentication server
- FIDO2 / WebAuthn support
- PKI integration
- Policy & risk engine
- Audit & reporting

Business Benefits:

- Centralized identity control
- Compliance readiness
- Scalability across environments
- Full audit visibility

Core Pillars

Frictionless, Passwordless Security

Provides seamless integration and secure access across all enterprise systems. Manage identities and authenticate users securely. Seamlessly integrates enterprise applications to deliver secure access, centralized identity management, and frictionless user authentication.

Inclusivity as a Security Strategy

Enterprise-grade security should be simple, intuitive, and accessible. InnaIT delivers a user-friendly authentication experience that enables people of all ages and technical abilities to securely access digital services with confidence.

Identity Governance and Administration (IGA)

Authentication answers the question of who a user is. Governance answers the equally important question of what that user should be allowed to access, and for how long. InnaIT extends its Zero Trust identity platform with Identity Governance and Administration capabilities that give organizations complete visibility and control over the entire identity lifecycle.

From the moment a user joins the organization to the day they leave, InnaIT automates provisioning, access changes, and de-provisioning across cloud, SaaS, and on-premises applications. Access rights are granted based on roles and policies, reviewed periodically through access certification campaigns, and revoked automatically when no longer required, closing the gaps that attackers exploit through orphaned accounts and excessive privileges.

Key Capabilities:

- Automated user lifecycle management (joiner, mover, leaver)
- Self-service access requests with policy-based approval workflows
- Periodic access certification and review campaigns
- Role-Based Access Control (RBAC) and Segregation of Duties (SoD) enforcement
- Orphaned and dormant account detection
- Centralized audit trails and compliance reporting

Business Benefits:

- Reduced risk from excessive privileges and orphaned accounts
- Faster, error-free onboarding and offboarding
- Audit readiness for RBI, GDPR, DPDPA, and other regulatory frameworks
- Lower administrative overhead through automation
- Complete visibility into who has access to what, and why

Behavioral Biometrics

Authentication is an event. Trust must be continuous. Behavioral biometrics makes this principle a reality by verifying identity not just at login, but throughout the entire session.

Every user interacts with devices in a way that is uniquely their own: the rhythm of their typing, the way they move a mouse, how they swipe and scroll on a touchscreen, and even how they hold their device. InnaIT analyzes these behavioral patterns passively and continuously in the background, building a dynamic profile of each legitimate user without adding any friction to their experience.

If a session is hijacked, a device is compromised, or credentials are misused by someone other than the intended user, behavioral anomalies are detected in real-time. The platform can then respond adaptively, triggering step-up authentication, restricting access, or terminating the session, stopping account takeover and fraud even after a successful login.

Key Capabilities:

- Continuous, passive identity verification throughout the session
- Keystroke dynamics, mouse movement, and touch-gesture analysis
- Real-time risk scoring and anomaly detection
- Detection of session hijacking, bots, and remote-access fraud
- Adaptive response with step-up authentication and session controls

Business Benefits:

- Continuous Zero Trust assurance beyond the point of login
- Reduced account takeover and transaction fraud
- Zero added friction for legitimate users
- Stronger protection for high-value banking and enterprise transactions
- Enhanced compliance with evolving fraud-prevention guidelines

Success Story

Passwordless Banking at Scale: Securing **120,000+** Users with Biometric MFA

When one of India's largest private sector banks needed to eliminate password-based risks and address RBI CSITE observations, Precision Biometric delivered a fully automated biometric MFA solution integrated with the bank's identity ecosystem.

The result:

120,000+
users secured

16× higher
throughput than required

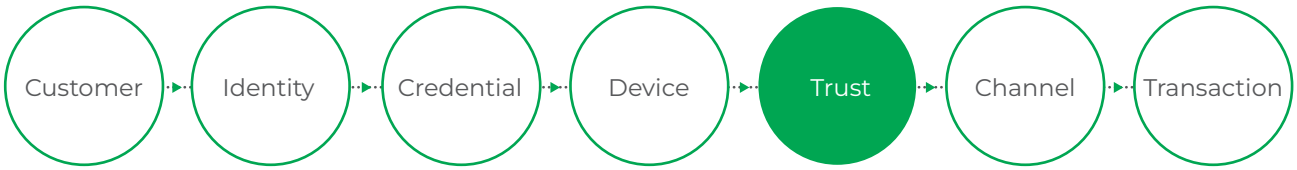
zero
unplanned downtime

Three
consecutive years of zero RBI CSITE and internal audit observations.

Our Client Portfolio:

State owned Public Sector Bank in North India	*Defence and Aerospace Electronics Company*	*Digital Payments Technology Company*
Indian Financial Services Conglomerate	*Fast-Growing Small Finance Bank*	*Global Digital Transformation Company*
Small Finance Bank	*Indian Private Sector Bank*	*Microfinance Institution in India*
Private Sector Bank in South India	*Regional Banking Institution in South India*	

How does it work?



Why Choose InnaIT?

- 100% Passwordless Authentication
- Hardware-backed identity protection.
- Biometric verification
- PKI-based digital signing
- FIDO2 & WebAuthn ready
- Enterprise SSO & MFA
- Centralized governance
- Cloud, Hybrid & On-Prem support
- Compliance ready
- Advanced audit & reporting

Business Impact

- Stronger security posture
- Reduced risk of breaches
- Improved user productivity
- Lower operational costs
- Simplified identity management

Secure the Future of Digital Identity

As digital transformation accelerates, identity has become a cornerstone of enterprise security. Organizations need more than traditional authentication. They need a trusted, passwordless identity platform that secures users, devices, applications, and transactions without compromising usability. InnaIT enables this shift by combining patented PKI and biometric technologies with Zero Trust principles to deliver secure, seamless, and phishing-resistant authentication.

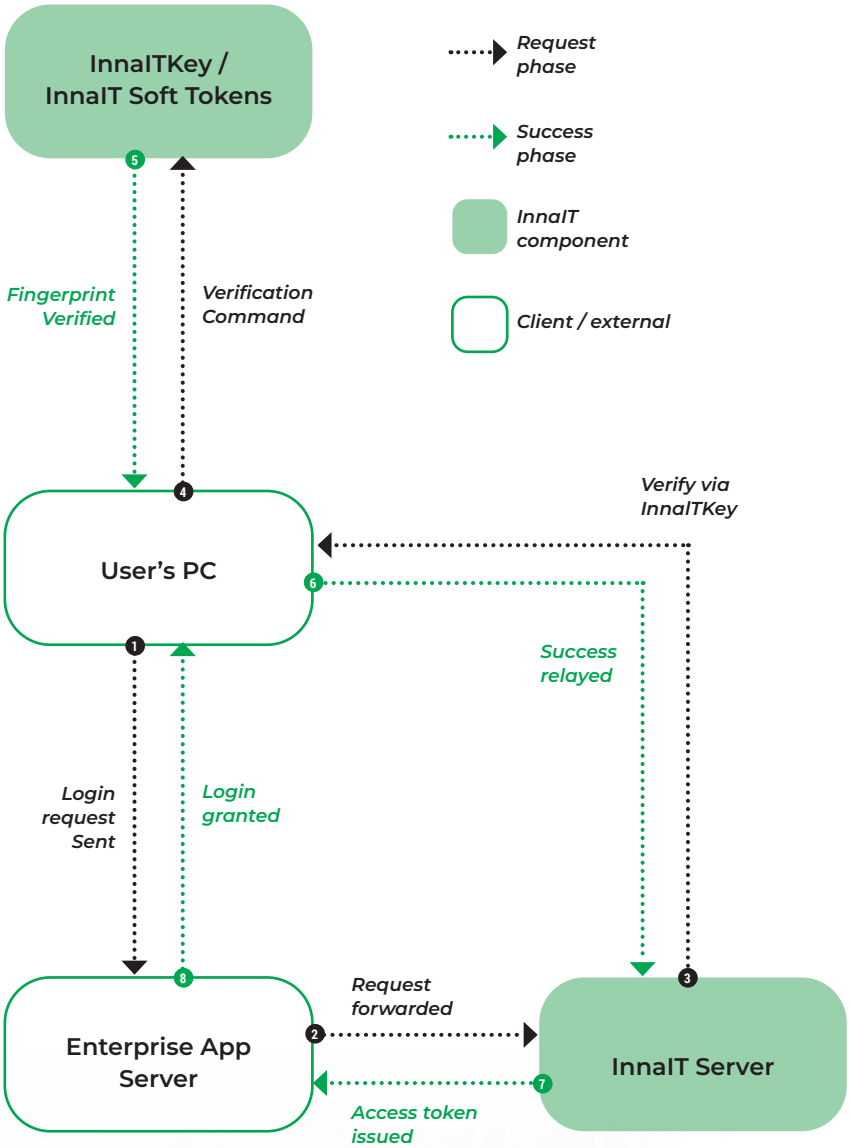
Built for modern enterprises, InnaIT provides a comprehensive identity and access management solution that simplifies administration while strengthening security across cloud, hybrid, and on-premises environments. From passwordless authentication and trusted digital signing to transaction authorization and centralized identity governance, InnaIT empowers organizations to confidently meet evolving security, compliance, and business demands.

With over three decades of expertise in secure identity solutions, Precision Biometric continues to help enterprises, financial institutions, and governments build trusted digital ecosystems. As organizations prepare for the future of cybersecurity, InnaIT stands ready to protect every identity, secure every interaction, and enable digital trust at scale.

Standards & Criteria

- FIDO2, FIPS 140-2/140-3, CERT-In Compliance, Common Criteria (CC EAL 6+)
- PII & Data Privacy Enabled
- Meets Global Regulatory Compliance
- Auditability & Scalability
- Authentication, Authorization & Non-Repudiation (AAN)

Flowchart representation of the InnaIT framework in action



PRECISION BIOMETRIC | InnaIT IDENTITY SECURED

Precision Biometric India Private Limited
22, 1st Floor Habibullah Road, T.Nagar, Chennai 600 017 | T: +91 44 4501 5000
Sales: **innaitdsc@precisionit.co.in** | Technical Support: **biometricsupport@precisionit.co.in**
https://www.precisionit.co.in | https://www.innait.com