Precision's InnaIT Key

Enterprise

Eliminate credential compromise

Eliminate password fatigue

Friction-less, Password-less

Unique user signature & Transaction audit trails

Precision's InnaIT[Key] PK1100 - Enterprises

A highly secure solution that innovatively combines PKI and Biometric to provide Passwordless Identity Authentication, Transaction Authorization and Signing InnaIT[Key] is a FIDO2 L2 certified biometric device which can be used for FIDO enabled authentication services including Microsoft Azure active directory.

OVERVIEW

InnaIT[Key] is a secure biometric device incorporating a best-in-class, highly secure anti-spoof fingerprint match-in-sensor and a high-end crypto controller that provides advanced asymmetric cryptography. The solution innovatively combines **PKI and Biometric** to provide **Passwordless Identity Authentication, Transaction Authorization and Signing** thus preventing **Credential compromise, Phishing attacks, Password fatigue and enables seamless multi-device use.** The solution thus contributes significantly to **Fraud reduction, enhanced User Experience, and increased Productivity.** InnaIT[Key] is a state-of-the-art offering that solves problems across various industry verticals like Enterprises, BFSI, Automobile, Share trading, Pharmaceuticals and more.

These are the Solutions InnaIT[Key] Provides

Organisation needs to ensure that only authorized users gain access to enterprise IT infrastructure and applications

InnaIT[Key] is designed with a high-end crypto controller that provides advanced **PKI (RSA up to 4096/ECC up to 521) asymmetric cryptography** to establish bi-directional trust and **strong biometric authentication** thereby ensuring that it is indeed a legitimate user that is logging in.

Users experience password fatigue and are also worried about their credentials getting compromised. They need a 'zero-trust' solution

InnaIT[Key] provides a **friction-less, passwordless** experience with secure biometric authentication and advanced asymmetric cryptography, thereby eliminating all possibilities of credential compromise and password fatigue.

Ease of integration with existing enterprise applications & elimination of impersonation

InnaIT[Key] provides biometric based login to **Windows AD with 2FA and Enterprise Single Sign-On methods**. This **eliminates impersonation**, as unique biometrics identify each user even if a common ID is used for login (system admin). **Audit trail** of the actions performed, with login timestamp makes it easy to keep track of user activity. Existing enterprise software (eg. SAP) and standards-based integration are made seamless with this solution. Also, **transaction level authorizations** are possible with customizable applications.

Users access enterprise IT infrastructure & applications through multiple devices like Mobile phones, Laptops and Desktops including company provided assets, BYOD on travel, WFH (Win logon/VDI/VPN access)

InnaIT[Key] is designed with the latest Biometric Match-in-Sensor and a high-end crypto controller can be **connected to any device**, thereby providing flexibility & convenience, while eliminating credential compromise and providing **secure end-to-end encryption** across multiple devices.

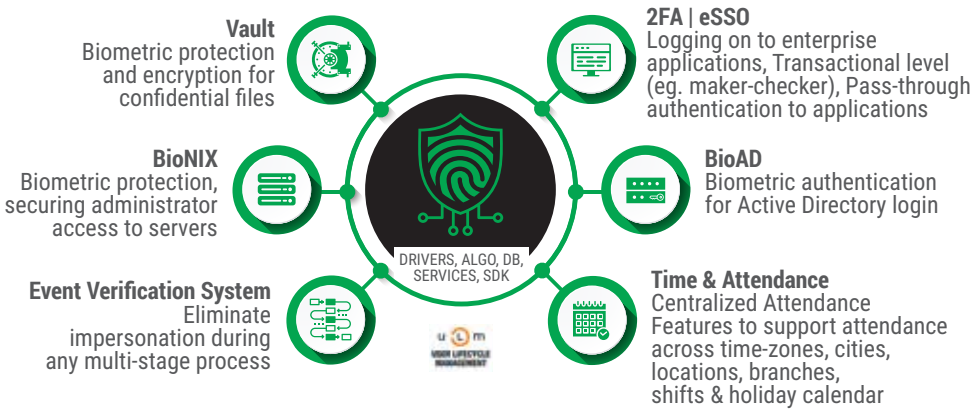
Transaction authorization accompanied by transaction signing with unique user signature and the need to compile Audit trails for Statutory purposes & Analysis

InnaIT[Key] provides biometric authentication based login, transaction approvals and additionally each transaction is encapsulated with the **unique user signature**, thereby rendering the access and transaction **non-repudiable**. The biometric authorization helps in maker-checker scenarios and the timestamp record during the authentication makes it easy to compile **audit trails** for statutory purposes & analysis.

Secure data storage with biometric access control

InnaIT[Key] complies with **encryption and signing** guidelines, documents can be stored securely within a **vault** and hierarchy-based access can be provided, mapping with users' biometric.

InnaIT Modules



Vault
Biometric protection and encryption for confidential files

BioNIX
Biometric protection, securing administrator access to servers

Event Verification System
Eliminate impersonation during any multi-stage process

2FA | eSSO
Logging on to enterprise applications, Transactional level (eg. maker-checker), Pass-through authentication to applications

BioAD
Biometric authentication for Active Directory login

Time & Attendance
Centralized Attendance Features to support attendance across time-zones, cities, locations, branches, shifts & holiday calendar

Comparison of Methods

Consideration	InnaIT[Key] PK1100	InnaIT[Key] PK1210	Software Token(Device – Mobile/Laptop with Biometric)	Mobile Authenticator
True Password-less Authentication	Yes (Prevents phishing attacks)	Not available	Possible (but not secure)	Not possible
Transaction Authorization	Possible	Not possible	Not possible	Possible
Transaction Signing	Possible	Possible	Possible	Not possible
Common Criteria Certification	EAL6+(high)	EAL6+(high)	None	None
True Random Number Generation (important aspect in generating keys for PKI)	TRNG that is AIS 20/31 PTG.2 compliant	TRNG that is AIS 20/31 PTG.2 compliant	Provider specific	Provider specific
Library used	Certified library for use inside Crypto controller	Certified library for use inside Crypto controller	Any	Provider specific
Biometric – Storage	Secure in sensor	Not available	Device-native biometric data stored on host (Security is model specific)	Might use device native biometrics
Biometric comparison	Quantum matcher Secure in sensor	Not applicable	Performed on host	As above
User identification	Absolute – Non-repudiable	Not applicable	Not certain	Not certain
Mapping of user to System	Possible	Not possible	Not reliable (as user identity is in question)	Depends on integration (not reliable as user identity is in question)
Spoof detection	Tested against 23 spoofs	Not applicable	Not applicable	Not applicable
Multi-device use (Mobile/Phone/ LT/DT)	Plug device into host and use	Plug device into host and use	Separate tokens to be generated for each host	Possible (Mobile device required)
Out-of-band channel	Available	Available	Not available	Available

Stakeholder Benefits

THE MANAGEMENT

- Robust Information Security
- Audit trails are legitimate
- Assignment of responsibility and non-repudiation
- Branding
- No privacy or compliance issues
- Financial Savings
- Secure solutions for the new normal

THE USER

- Prevention of impersonation
- Secure access to all services
- Elimination of password fatigue
- Ability to freely 'Roam'
- Convenience

THE IT TEAM

- No need for centralized biometric database
- Time, effort and cost optimization
- Ease of Deployment & Administration
- Significantly reduced administrative overhead
- Information Security

InnaIT[Key] SPECIFICATION PK1100

PRECISION GROUP

OVERVIEW :

InnaIT[Key] is a secure biometric device incorporating a best-in-class, highly secure anti-spoof fingerprint match-in-sensor and a high-end crypto controller that provides advanced asymmetric cryptography. Together with the server stack and SDK, the solution eliminates credential compromise, enables multi-device use and end-to-end encryption. InnaIT[Key] is a state-of-the-art offering that solves problems across various industry verticals like Enterprises, BFSI, Automobile, Share trading, Pharmaceuticals and more.

HIGHLIGHTS :

- Security System on Chip (SoC)
- Biometric Match in Sensor
- Unique Signature
- End-to-End Solution H/W & S/W Integration

fido CERTIFIED L2 FIDO2

SPECIFICATION

	Category	Nominal Value
1	**GENERAL SPECIFICATION**	
a	Certification	FIDO2 L2
b	Operating Temperature	0°C to 85°C
c	Operating Voltage	5V, 100mA DC
d	Connectivity	USB Type-C 2.0
e	Indication	Tri-Colour LED
f	ESD	IEC61000-4-2 Air Discharge +/- 8KV
2	**MICRO CONTROLLER**	
a	Controller	Infineon SLE78
b	CPU	Self-checking dual CPU with Integrity Guard™
c	Certifications	Common Criteria EAL 6+ (high) EMVCo
d	Asymmetric Cryptography	ECC up to 521-bit RSA up to 4096-bit
e	Symmetric Cryptography	AES 256-bit
3	**SENSOR SPECIFICATION**	
a	Sensor	Synaptics MIS; High performance sensor with hardware accelerated ultra-fast match time
b	Sensor type	Capacitive
c	Package Size	10.87mm x 10.87mm
d	DPI	363DPI
e	Security	Hardware accelerated security engine for end-to-end security
4	**MECHANICAL**	
a	Device Dimension	H 32mm, W 19mm, T 5.20mm
b	Material type	ABS
c	Device Weight	20g

PRECISION BIOMETRIC

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