Precision's InnaIT Key

Government

Establish
Bi-Directional Trust

Eliminate Phishing &
Man-in-the-Middle attacks

Convenient
On-The-Go Device

Precision's InnaIT[Key] PK1100 - Government

A highly secure solution that innovatively combines PKI and Biometric to provide Passwordless Identity Authentication, Transaction Authorization and Signing

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 Government departments, BFSI, Automobile, Share trading, Pharmaceuticals and more.

These are the Solutions InnaIT[Key] Provides

The defense/federal institution finds it challenging to identify its legitimate user with absolute certainty

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 are unable to ensure that they are connected to the authentic institution (prey to Phishing attack) 'zero-trust'

InnaIT[Key] solution adopts a hardware-based PKI (RSA up to 4096/ECC up to 521) asymmetric cryptography to **establish bi-directional trust** that ensure that the user is connected to the authentic institution's servers and not to a phishing site.

Man-in-the-Middle attack

After ensuring bi-directional trust, InnaIT[Key] solution implements **AES 256 symmetric encryption** methods that carry unique identifiers and timestamps to eliminate possibility of man-in-the-middle attacks.

Any existing OTP method using Mobile number for transaction approval is not secure and incurs recurring costs

InnaIT[Key] adopts the latest **System on Chip design-based Match in Sensor** biometric authentication with built in anti-spoof protection, ensuring that the transaction is not compromised thus eliminates the need for OTP based approvals and thereby the costs, forever.

Users use multiple devices like Mobile phones, Laptops and Desktops (@Home)

InnaIT[Key] solution designed with the latest Biometric Match in Sensor and a **high-end crypto controller** can be connected to any device and thereby eliminates credential compromise and provides secure end-to-end encryption across multiple devices.

Every transaction is not accompanied by a unique user signature

InnaIT[Key] solution implements 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**.

Comparison of Methods

Consideration	InnaIT[Key] PK1100	InnaIT[Key] PK1210	Software Token(Device – Mobile/Laptop with Biometric)	Mobile Authenticator	OTP
True Password-less Authentication	Yes (Prevents phishing attacks)	Not available	Possible (but not secure)	Not possible	Not possible
Transaction Authorization	Possible	Not possible	Possible	Possible	Possible
Transaction Signing	Possible	Possible	Possible	Not possible	Not possible
Common Criteria Certification	EAL6+(high)	EAL6+(high)	None	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	Provider specific
Library used	Certified library for use inside Crypto controller	Certified library for use inside Crypto controller	Any	Provider specific	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	Not applicable
Biometric comparison	Quantum matcher Secure in sensor	Not applicable	Performed on host	As above	Not applicable
User identification	Absolute – Non-repudiable	Not applicable	Not certain	Not certain	Not certain
Mapping of user to System	Possible	Only device can be mapped	Not reliable (as user identity is in question)	Depends on integration (not reliable as user identity is in question)	Not possible
Spoof detection	Tested against 23 spoofs	Not applicable	Might use device native biometrics	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)	Possible
Out-of-band channel	Available	Available	Not available	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 IT TEAM


No need for centralized biometric database


Time, effort and cost optimization


Ease of Deployment & Administration


Significantly reduced administrative overhead


Information Security

THE USER


Prevention of impersonation


Secure access to all services

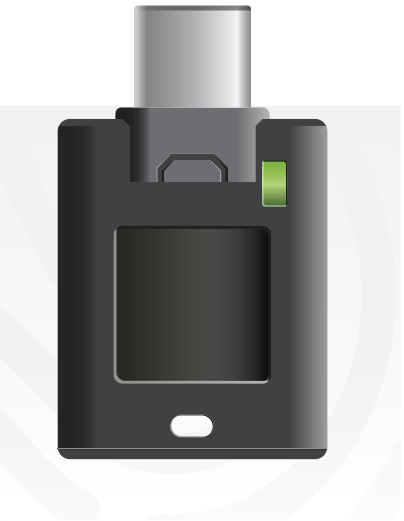

Elimination of password fatigue


Ability to freely 'Roam'


Convenience

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 Government departments, 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

SPECIFICATION

	Category	Nominal Value
1	**GENERAL SPECIFICATION**	
a	Operating Temperature	0°C to 85°C
b	Operating Voltage	5V, 100mA DC
c	Connectivity	USB Type-C 2.0
d	Indication	Tri-Colour LED
e	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, FIDO2 L2
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**