Precision's InnaIT[Key] PK1100

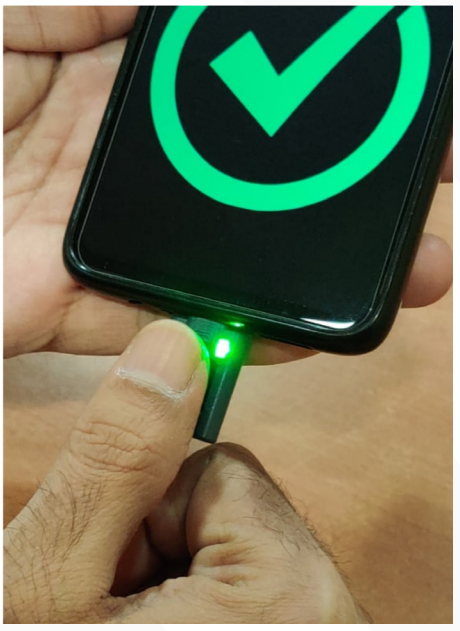
PRECISION GROUP

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

These are the solutions InnaIT[Key] provides

Bank is unable to identify its customer 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 genuine customer that is logging in.

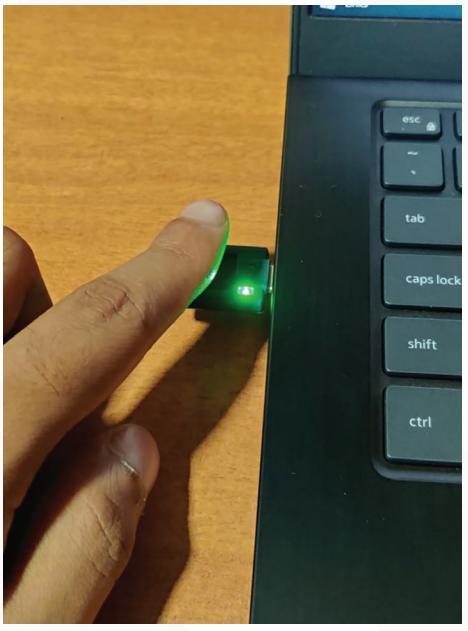


User is unable to ensure that they are connected to the Bank (prey to Phishing attack)

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 bank 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.



Existing OTP method using Mobile number for transaction approval is not secure and incur 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.

Customers 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 customer signature

InnaIT[Key] solution implements biometric authentication- based login, transaction approvals and additionally each transaction is encapsulated with the **unique customer signature**, thereby rendering the access and transaction **non-repudiable**.

PRECISION GROUP

Stakeholder Benefits – The Management

Robust Information Security
Solution provides exceptionally high levels of security and helps implement robust IS practices

Audit trails are legitimate
Since user biometrics exist only on the InnaIT[Key] which is in the users' possession only

Assignment of responsibility and non-repudiation
Ability to identify specific user, on account of biometrics, who carried out specific actions and elimination of deniability

Branding
Precision can provide customized InnaIT[Key] designs with Organization's brand elements

No privacy or compliance issues
Since user biometrics exist only on the InnaIT[Key] which is in the users' possession only

Time, effort and cost optimization
No more wasted time and effort in the IT Function with issues like forgotten passwords and resets

Financial Savings
On account of reduced fraudulent transactions, reduced service incidents, reduced IT admin manpower requirements, reduced need for Service Desk manpower

Secure solutions for the new normal
Can enable new secure solutions for WFH scenario

Stakeholder Benefits – The User

Prevention of impersonation
Solution provides exceptionally high levels of security and helps implement robust IS practices

Secure access to all services
From attendance to OS login to enterprise application authentication

Elimination of anxiety associated with centralized storage of biometric features
Biometrics never leave the device, which is specific to user

Elimination of password fatigue
User logs in with fingerprint and not with a username and password

Ability to freely 'Roam'
Use the same device on all endpoints without having to be 'tied' to a/some specific device(s)

Convenience
Small form factor device which can be attached to a key-ring. Connect to endpoint and use

Secure solution
A misplaced or stolen InnaIT[Key] can never be used by anyone else

Stakeholder Benefits – The IT Team

Reliable authentication
Authentication is based on biometrics which are unique to the user

No need for centralized biometric database
Biometric data is stored on InnaIT[Key] issued to user and nowhere else

Information Security
Eliminates information security issues related to compromised passwords

Ease of Administration
Virtually no additional administration efforts after issuing the InnaIT[Key] to the user

Prevention of impersonation
Unlike in a password-based system, credentials cannot be compromised, and proxy logins are eliminated

Significantly reduced administrative overhead
No more forgotten passwords and resets resulting in saved time and effort

Non-repudiation
Eliminates the possibility of repudiation since authentication is based on an individual's biometrics

Ease of deployment
Easy to deploy solutions with all components and implementation from a single source

PRECISION GROUP

Comparison of methods | RSA Token

RSA SecurID Tokens

- Combine 'what you know' (PIN) and 'what you have' (token code – 6 or 8 digit pseudorandom number that changes at specific intervals)
- Employ AES and are time synchronous
- Seed number unique to the individual token + current elapsed time + hash = code
- Hardware Token: Generates token codes using built-in clock & factory encoded random key
- Software Token: Require application specific to the intended device platform (OS/Phone/Computer). User obtains symmetric key and application generates token on the device. Same functionality as hardware token

Vulnerabilities

- Hardware tokens can be stolen or lost
- Soft tokens reside on a device and the device can be lost or stolen
- Vulnerable to breach of codes and man-in-the-middle attacks

Comparison of methods | OTP

OTP

- Combine 'what you know' (password) and what you have (OTP sent to a device – SMS and/or email)
- Randomly generated numeric code at each authentication event
- Present implementations – TOTP (Time based OTP) - Generated using current time and combines with a secret key
- Can provide two-factor authentication at login or single-factor at transaction
- Use 'Out-of-band' channels – SMS or email
- Other variants: Split OTP, Call-back OTP etc.,

Vulnerabilities

- Device compromise: Device which receives OTP can be lost or stolen
- Breaches could be caused by SIM cloning
- Social engineering can cause breaches
- OTPs are usually 'pseudo-random' and hence hacking algorithms can repeat the sequence and 'guess' the next OTP

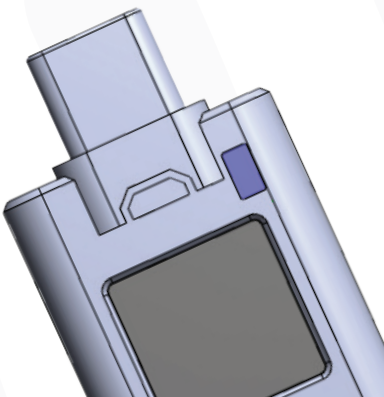
Comparison of methods | PKI Token

PKI Hardware Token

- Combine 'what you know' (Password) and 'what you have' (PKI Hardware Token)
- Store digital certificates and private keys
- Certificates are issued by a CA and bind keys with identities
- Used for authentication, encryption and digital signatures
- Use RSA & AES for asymmetric & symmetric encryption respectively
- USB or NFC options

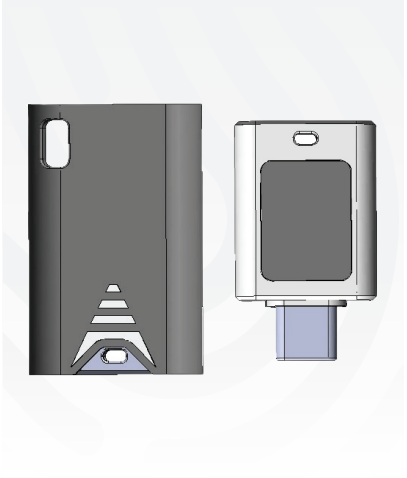
Vulnerabilities

- Hardware tokens can be stolen or lost
- User authentication without consent
- Remote usage of PKI enabled devices by hackers
- Lack of secure I/O channel between device and NFC based token card



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 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
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**