E3-P1 PIN Pad Provides the Highest Degree of Security Available ... With No Extra Fees

Heartland Payment Systems®, one of the nation's largest payments processors, leveraged its unique experience and knowledge to develop E3 end-to-end encryption. E3 technology protects your customers' credit and debit card data.

With E3, you get the strongest security solution available that:

- ☑ Protects cardholder account data from the moment of card swipe or key entry and through the Heartland network — not just at certain points of the transaction flow.
- ☑ Features layers of security using software and tamper-resistant hardware, as well as Advanced Encryption standard (AES) — the most secure encryption available.
- ☑ Ideal for protecting manually entered credit card numbers when processing mail orders and telephone orders.

Implementing and maintaining E3 to protect your business is easy and cost-effective. E3:

- ☑ Doesn't require changes to your daily routine or business processes.
- ☑ Offers fast transaction speed.
- ☑ Saves you time and money by automatically changing encryption keys — so you don't have to.
- ☑ Significantly lowers the cost of PCI compliance and the risk of being non-compliant.

To learn more about how implementing E3 achieves this, visit E3secure.com.

Heartland does not charge extra fees and taxes for this state-of-the-art security.

Unlike other processors and equipment manufacturers who charge additional fees to keep you secure, Heartland does not charge any extra fees or encryption taxes for this state-of-the-art security. We invested millions of dollars to develop this technology with the belief that you shouldn't have to pay more to be secure. That's why there are no added transaction fees, no monthly encryption fees, no key management fees, no activation fees, no insurance fees — or any other "junk" fees that may not bring you any extra value.

We so strongly believe in the ability of E3 to protect card data that we stand behind our encryption solution with our E3 Encryption Warranty.

Should transactions protected by E3 be breached using our E3 technology we will reimburse your breach related fines.*

* *Reimbursement is subject to the terms and conditions of Heartland's "E3 End-to-End Encryption Warranty." For more details, visit E3secure.com*

E3 Pin Pad

E3-P1 PIN Pad Technical Specifications

Marketing Name	Heartland E3 PIN Pad
Model Name	HPSE3-P1-DB9 (DB9 serial connector) HPSE3-P1-USB (USB connector) HSPE3-P1-RJ11 (RJ11 connector/ appropriate for E3 terminals)
Manufacturer	Heartland Payment Systems
Supported Payment Host	Exchange
Supported Settlement Host	Passport
Micro controller	32-bits processor (MIPS 4KSd architecture running at 96MHz)
Memory	Inside CPU: 128KB SRAM, 256KB Flash, with 512bit Battery backup key register External: 128KB SRAM, 2 MB flash
Display	4*16 characters LCD display; full ASCII set characters display capability. Backlight is optional.
Key Pad	16 keys keypad. The digit keys are randomly scanned.
PIN encryption	1. Follows ANSI X9.8 for PIN block and National Bureau of Standard DES / Triple DES algorithm in Electronic Code Book mode. 2. EMV level 2 specified PIN block with RSA encryption (maximum 1984bits mod).
PIN/Debit Key management	1. Master/ Session key (MK/SK). 2. Unique Key per Transaction conforms to ANSI X9.24-1992 and 2002. (MK/SK and DUKPT is mutual exclusive, different message format needed). 3. Certification Authority Public Key.
Message Frame	Compatible to VISA specifications.
Interface	[USB] B-Type Connector. [RS232] Six-position RJ-11 Connector (to DB9 RS232 connector). Preset to: 9600 BPS, 8 bits per character, none parity, one stop bit. (Null modem to PC)
Power	Regulated +5VDC input, 150mA (typical); 500mA (max.).
Battery Life	5 years for Security Data backup.
Diagnostic	Self-diagnostic includes MCU, Program checksum, Key checksum, Buzzer.
Dimension	168mm (L) x 100mm (W) x 48.5mm (H) without privacy shield
MSR Option	ISO7811, 3 tracks.
Smart card reader	ISO7816-1, 2, 3 and EMV 2000 level 1 compliant. Reads T=0, T=1 cards. Have one primary and three SAM card interface.

Integrations

- E3-P1 integrates with the E3 terminals as a secure PIN entry device
- E3-P1 specs are available for integration with third party integrated POS and Virtual POS systems

Approvals

- PCI PED 2.x

Security

- Hardware-based encryption protected by a Tamper-Resistant Security Module (TRSM)
- E3 data encryption key automatically updates upon every 50 swipes, every 24 hours, and at power-up
- Tamper-Resistant Security Module (TRSM)
- Because of Identity-Based Encryption (IBE), E3 devices self-generate cryptographic keys—meaning there is no key management required for you
- E3 data encryption utilizes AES 128-bit format-preserving encryption to protect sensitive card data