



HEARTLAND PAYMENT SYSTEMS' E3™ TECHNICAL INSIGHTS

IS E3 TRUE END-TO-END ENCRYPTION?

Heartland Payment Systems has a unique perspective on end-to-end encryption. We believe true end-to-end encryption is defined by the points where the encryption — or scrambling — of payment account numbers (PANs) starts and ends.

With E3, encryption begins the moment of card swipe and through the Heartland network. This includes four zones of the card processing ecosystem:

1. From data entry/card read at a business location to the payments processor's authorized network;
2. From entry to that network and throughout the entire processor/sub-contractor network where data is in motion;
3. While the data resides in a central processing unit (CPU) or a host security module (HSM). An HSM is a specialized server that locks down information;
4. In storage — data at rest.

Any encryption solution that does not start at the card swipe and include all of these four zones is not end-to-end according to our definition of end-to-end but may be "point-to-point encryption." Point-to-point solutions protect data at certain points in the lifecycle of a transaction flow — and expose them at others.

DOES E3 RELY SOLELY ON SOFTWARE TO PROTECT THE DATA?

No. E3 features layers of security using both software and Tamper-Resistant Security Modules or TRSMs. Unlike other solutions, E3 does not rely solely on software to safeguard sensitive data because software can be hacked. Protection by both is essential for helping merchants reduce their Payment Card Industry (PCI) compliance burden and building the confidence of cardholders.

DOES E3 LEVERAGE THE STRONGEST ENCRYPTION AVAILABLE?

Yes. E3 uses 128-bit-strong Advanced Encryption Standard mode encryption — also known as AES. AES is a protocol required by the United States Government and is the most secure encryption available. It is the first publicly accessible and open encryption approved by the National Security Agency for top-secret information.

WHAT DATA IS PROTECTED?

E3 encryption protects the PAN — whether read from a payment card's magnetic stripe or manually entered — before the application on the device can access it, and protects the full Track 1 and 2 data in transmission to the host. By doing this, the full PAN and track data are never available to the application or the merchant's point-of-sale (POS) system. Account information is protected by Format-Preserving Encryption (FPE) and soon, tokenization.

HOW DOES THE CARD NUMBER APPEAR ON THE RECEIPT AND REPORTS?

FPE does not alter the format of the data once it is encrypted. For example, a 16-digit card number will still look like a 16-digit number. FPE allows access to the first six and last four digits of the card number while encrypting the intermediary digits of the card number, enabling receipt printing and the ability to manage returns.

HOW ARE ENCRYPTION KEYS MANAGED?

E3 devices do not require remote or on-site injections (downloads) to change the keys that encrypt the data. Once deployed, E3 devices — including terminals and wedges — leverage Identity-Based Encryption (IBE) technology so they never have to be "touched" to update the E3 encryption keys. This significantly reduces the cost and administration efforts while increasing security for merchants using E3.



HOW DOES E3 ENCRYPTION COMPARE TO TOKENIZATION?

With tokenization at the point of sale in software, cardholder data is replaced with a marker — or token — in the merchant's system. While tokenization prevents the theft of data in storage, sensitive transaction data remains vulnerable at the point of sale and during transmission.

Tokenization is a benefit when paired with encryption ensuring data is initially protected at the point of sale and in transmission ... as well as in storage.

WILL THE E3 DEVICES WORK WITH OTHER PROCESSORS?

No. The E3 devices are built on Heartland's state-of-the-art encryption architecture and work only when a merchant processes with Heartland.

DOES THE E3 TERMINAL SUPPORT OTHER PAYMENT APPLICATION SOFTWARE?

No. E3 terminals only support payment applications cryptographically signed and authenticated by Heartland. Third-party software is not supported, which provides another level of security that prevents rogue or malicious software from being installed on the E3 terminal.

DOES THE E3 TERMINAL SUPPORT PIN DEBIT?

Yes. There is an internal PIN pad that can be used for PIN debit transactions.

CAN I USE AN EXISTING EXTERNAL PIN PAD?

Because of the TRSM and secure data lines, only the internal PIN pad can be supported at this time.

HOW DURABLE IS THE E3 TERMINAL?

Terminal durability is comparable to — or better than — other major brands. The terminal comes with an industry-standard 12-month warranty and will soon be certified by PCI under its Pin Entry Device (PED)/Pin Transaction Security (PTS) standards.

WHAT DO I HAVE TO DO DIFFERENTLY TO USE THE E3 TERMINAL?

Absolutely nothing! There are no changes to a merchant's daily routine or speed of transactions. Plus, the menus are simple, familiar and intuitive.

To learn more about E3 and protecting cardholder data, contact your Heartland relationship manager or account manager — and visit E3secure.com. You can also contact Heartland at 866.941.1HPS (1477).



866.941.1HPS (1477)
HEARTLANDPAYMENTSYSTEMS.COM
E3SECURE.COM

