



The Highest Standards | The Most Trusted Transactions

Heartland End-to-End Encryption Whitepaper

1. The Heartland End-to-End Encryption Security Model

The Heartland end-to-end encryption security model is being designed to protect sensitive payment account and processing data from unauthorized access and to render data unusable if improperly accessed.

As presently envisioned, the model will deploy:

- Data encryption to render data inaccessible in clear text format from the point of card swipe and when manually entered via a Pin Entry Device (PED) keypad
- Tamper Resistant Security Modules (TRSM) on encrypting devices to protect cryptographic secrets
- Hardware Security Modules (HSMs) within Heartland's processing network for protecting cryptographic secrets
- Physical access protections on devices to make data inaccessible to unauthorized users

1.1. What Will Be Protected?

Sensitive payment account and processing data that includes:

- Payment Account Numbers (aka Primary Account Number or PAN) of both credit and debit accounts, read from a card's magnetic stripe¹
- Entire Track 1 and Track 2 magnetic stripe data (which includes the PAN, expiration date, service code and Discretionary data) of both Credit and Debit cards

1.2. What is End-to-End?

"End-to-End" describes the concept whereby sensitive payment account data is protected from the point where data is captured . . . through all intermediary processes . . . and to the final credit issuer or debit gateway endpoint.

¹ Encryption of manually entered payment account data is also supported on devices with integrated PED (Pin Entry Device) keypads.

Only by completely removing the sensitive data, such as the payment account number, so it is never accessible in a usable format to the device application or the merchant and processor systems can the solution be called true “End-to-End Encryption.”

1.3. How Does Encryption Apply?

Encryption is the process of transforming information (referred to as plain text) using an algorithm (called a cipher) to make the information unreadable to everyone except those possessing special knowledge usually referred to as a key.²

Heartland’s end-to-end encryption security model as currently designed will require transforming sensitive payment account and processing data using encryption at card swipe and manual entry— and continuing to protect the data as it flows through Heartland’s processing platforms.

Heartland’s end-to-end encryption security model as currently designed will employ encryption to protect data “in flight” and data “at rest”. Data “in flight” is data that passes between systems in the processing flow. Data “at rest” refers to stored information usually as a result of processing activity.

Heartland describes the inter-relationship of the end-to-end components that employ encryption to protect sensitive payment account data as “Payment Zones.”

1.4. Heartland Payment Encryption Zones

Payment encryption zones refer to the computing operations and processes that operate under the same encryption parameters.

Heartland identifies five payment encryption zones in the payments cycle:

Zone 1: From data entry/card swipe at the merchant device to the authorization network gateways

Zone 2: Authorization network gateways

Zone 3: All points in which data is in motion within the computing network(s) of the processor

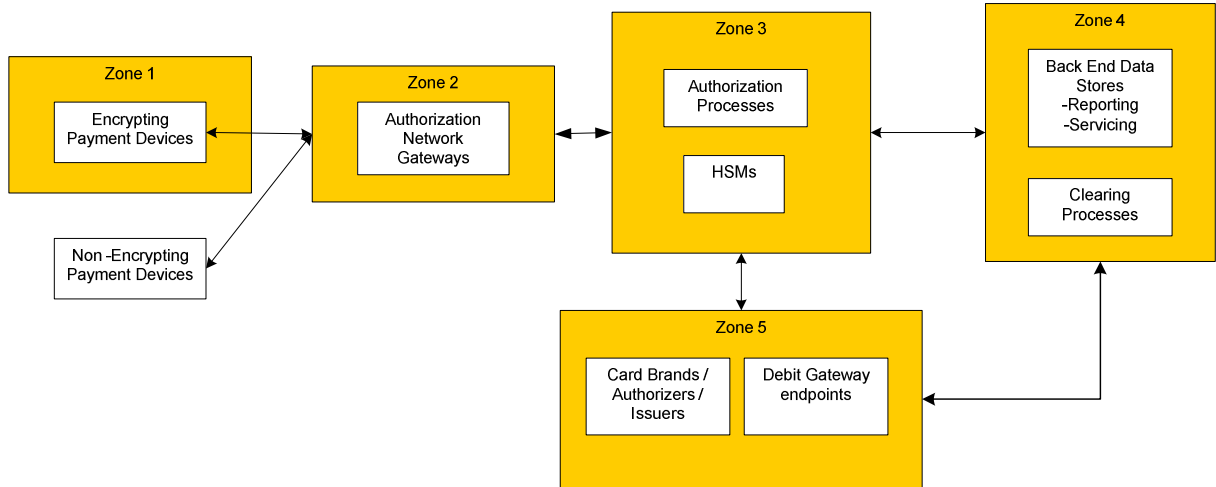
Zone 4: Back-end data storage that supports servicing and reporting. (Data at rest)

Zone 5: From the processor to the authorization center of the brand or issuer for authorization and settlement.

The following sections of this document describe the Heartland end-to-end encryption security model as currently designed by each payment encryption zone.

² The Free On-line Dictionary of Computing, © 1993-2007 Denis Howe, www.foldoc.org & PCI-Portal.com
<http://www.pci-portal.com/lang-en/component/directory/category/23>

Heartland Payment Encryption Zones:



2. Payment Encryption Zone 1: Securing Data from the Point of Entry

2.1. Devices That Read Magnetic Stripe Data or Accept Manual PAN Entry

For devices that read payment card magnetic stripe data or accept manual PAN entry and support encryption, Heartland's end-to-end encryption security model will — at a minimum— require that:

- Applications on the device never see full payment account number data
- The payment account number and payment card track data are transmitted fully encrypted from the device to the processor
- The device employs a Tamper Resistant Security Module (TRSM) with active tamper responses to protect encryption keys
- The device employs physical protections so tampering with the magnetic stripe reader (MSR) or data lines provokes an active response that wipes encryption key data from the device's secure processor and renders the device non-functional
- Devices that accept debit cards employ a secure MSR with an integrated pin pad
- For secure manual PAN entry, the device keypad must be under control of the TRSM. (This is the same manner in which debit PINs entry is protected.)

2.2. Payment Application Middleware

Payment application software implemented on a personal computer does not share the inherent physical security of a device designed specifically for payment processing.

For payment application software implemented on a personal computer—such as a virtual payment terminal— Heartland's end-to-end encryption security model will require the use of a secure MSR device that follows the same minimum attributes listed under section 2.1.

3. Payment Encryption Zone 2: Processor Authorization Network Gateways and Earliest Point Encryption

To protect the data during its transition from payment encryption zone 1 to payment encryption zone 2 requires Hardware Security Modules (HSM). HSM are specialized computer platforms that employ physical and logical protections to support secret cryptographic operations in the most secure manner available.

Heartland's end-to-end encryption security model will require that applications never receive data in plain text during transition between payment encryption zones that are under the complete control of Heartland.

For transactions originating from non-encrypting points—such as devices that do not support encryption, payment application middleware or manually entered account data from keyboards not equipped with encryption capabilities—Heartland will apply encryption to the sensitive data of the transaction at the earliest point possible. This data will be encrypted as an operation under payment encryption zone 2.

4. Payment Encryption Zone 3: Processor Operations

This zone represents the systems and subsystems that comprise core authorization processing. A significant operation in payment encryption zone 3 is the exchange of data with payment account issuers and gateways for authorization processing. HSM are leveraged to ensure the highest level of data security during processing for these operations

5. Payment Encryption Zone 4: Back-End Processor Clearing Environment and Data Storage

Data that has passed through payment encryption zone 3 and completed the authorization processing moves to payment encryption zone 4. The special characteristics of the data in this zone derive from the business operations that rely on sensitive payment account data being available for the clearing process and account servicing. HSM are leveraged for these operations to ensure the highest level of data security.

6. Payment Encryption Zone 5: Authorization and Clearing Processes to Third Party End-Points

Within payment encryption zone 5, sensitive payment account data is exchanged with authorization and clearing end-points such as the major card brands and debit gateways. Various methods of security and encryption will be employed to continuously protect the data "in flight" and "at rest" that passes from Heartland controlled payment encryption zones 3 and zones 4 to payment encryption zone 5.

7. Heartland's End-to-End (E3) Implementation

Heartland's end-to-end encryption solution, called "E3™", is designed to introduce recognized, cutting-edge encryption technologies into payment devices in a manner Heartland believes has never before been deployed. This will result in an elegant integration of encryption across the payment transaction life cycle.

Heartland believes innovative key management and utilization of the most advanced and accepted encryption technologies available will distinguish Heartland's E3 from other evolving solutions. The Heartland approach to E3 will seek the highest degree of security in efforts to establish a gold standard of encryption deployment.

7.1.1. Innovative Key Management

Heartland's E3 implementation is intended to enable each device to generate data encryption keys dynamically. Heartland will not have to inject keys to the terminal after the initial manufacturing, and keys will rotate without the need to further "touch" the device or remotely inject new keys. This method is expected to remove the headache and overhead of administering secure rooms, key injection facilities and paying fees for key injection services. Also, with this method, it is expected that no database of keys or index of tokens will be required to reside anywhere.

It is intended that every transaction from a Heartland E3 device will be secured by Advanced Encryption Standard (AES) encryption. No two devices will share the same keys, and data encryption keys will typically be updated daily without the need to be injected or call a host for a key update.

7.1.2. Highest Protections

While Heartland will support multiple encryption schemes, the Heartland E3 implementation has been designed to improve upon existing accepted encryption methods and key management.

E3 is designed to incorporate symmetric and asymmetric cryptography and employ modes of the AES algorithm. This algorithm has been recognized by the National Institute of Standards and Technology as an approved symmetric encryption algorithm that may be used by the US Government.³

As a point of clarification, the E3 implementation is not expected to rely on key management methods such as Master/Session or Derived Unique Key per Transaction (DUKPT). The E3 model will not require the device and the host to pre-share keys. The device generates its own keys and transmits the key wrapping information to the host using an asymmetric method.

8. Summary

As a processor, Heartland has a particular perspective and incentive to build a true end-to-end encryption solution that eases the pain for merchants deploying encrypting devices, increases the confidence of cardholders and increases data security throughout our processes.

Here is a checklist for comparing the E3 solution Heartland currently intends to implement to currently known competitors:

1. ***Is it true end-to-end encryption?*** Heartland's E3 will start where the data is entered and will not rely on software to protect sensitive data because software can be hacked. Heartland E3 devices will utilize physical and logical protections such as the Tamper Resistant Security Module to protect encryption keys and processing. This is also essential for helping merchants reduce their PCI compliance burden and building the confidence of cardholders.

³ National Institute of Standards and Technology; <http://csrc.nist.gov/groups/ST/toolkit/documents/aes/frn-fips197.pdf>

2. ***Is the strongest encryption available being leveraged?*** Heartland's E3 will use AES mode encryption.
3. ***What is being protected on the device?*** Heartland E3 will encrypt the payment account number either read from a magnetic stripe or manually entered through a keypad supporting encryption before any application on the device can access it. Therefore, the full payment account number will never be available to the application or the merchant's point-of-sale system.
4. ***What is being protected in transmission?*** Heartland E3 will encrypt the entire track data in transmission.
5. ***How are keys managed?*** Heartland E3 devices will not require any key injection, neither remotely or on-site. The devices will never have to be "touched" once they are deployed to update the E3 encryption keys. This will significantly reduce the cost and administration effort for merchants deploying a Heartland E3 device.

Author: Heartland Payment Systems

For further information and contacts please visit: www.E3Secure.com

Release Date: October 23, 2009



The Highest Standards | The Most Trusted Transactions