



# Host Security Module Integration Considerations

June 26, 2007

## Background

Small retailers that accept credit and debit cards use terminals provided by their banks. Larger retailers develop payment processing systems and networks to consolidate electronic payment transactions, so they can have more operations control and negotiate better rates for payment processing services.

A large retailer who accepts PIN-based debit cards needs to consider installing a Host Security Module (HSM) within his own systems. HSM installation allows the retailer to securely manage consumer PIN acquisition and translation within the retailer's internal systems, and simplifies his connections to his payment processing partners. This paper is offered to provide understanding of HSM function and implementation considerations.

Mustang MicroSystems, Inc. has provided consulting services to a number of retailers who were implementing PIN-based debit processing. Our services bring knowledge about HSMs and their operation, and we can lead retailers through the process of security compliance. Mustang is also a registered ESO (Encryption Service Organization). We provide key injection and payment terminal management services to a number of major retailers.

## HSM Considerations

Installation of an HSM assumes that the retailer has a payment network in place where payment transactions are consolidated and a network connection from that point to one or more payment processors. This function is often described as a payment transaction switch, and it includes both on-line transaction processing and daily cash settlement.

Retailers may already accept PIN-based debit. If the retailer does not have an internal HSM, he has a relationship with a processor that requires encryption keys in the retailer PIN-pads. Those keys are provided by the processor.

The HSM allows separation of PIN security within the store systems from the processors. With an internal HSM, the retailer controls the domain from the POS payment location to the payment gateway. The retailer controls all of the encryption process from the POS to the HSM, where encryption and decryption of PINs allows isolation of PIN security. The HSM provides the functions of encryption translation between the store systems and the links to the payment processors.

## Planning Considerations

Retailer installation of an HSM involves issues in business, technology, and security. Assuming that the business case is positive, the retailer needs to consider the following:

### ***What are HSM hardware options, and what should we use?***

There are three proven sources of HSM hardware and support in the United States. Mustang can provide current information.

### ***Where are the HSMs to be physically located?***

HSMs are rack mounted hardware devices about the size of a desktop PC. They are typically installed within the retailers secure data centers, usually in the network data center. Larger retail systems will also equip

their Disaster Recovery centers. Due to security requirements, another HSM is usually dedicated to development, and isolated from the secure HSMs.

***How do HSMs interface to retail systems?***

HSMs typically connect using standard IP / Ethernet. HSMs have a set of common application level messages and commands. All HSMs are similar in function, and support a set of industry standard commands. Once security is established and the HSMs are operational, there is little or no direct user contact.

***What encryption knowledge is needed?***

Knowledge for design and implementation of HSMs is commonly available, and other than the internal security processes, is very straightforward. HSMs work with specific data elements in financial transaction messages, decrypting and re-encrypting that data completely within the HSM hardware.

***What encryption keys are needed?***

A TDES DUKPT or Single DES DUKPT key is needed for the links between the retailers' POS PIN-pads and the HSM. TDES Master/Session Keys are provided by the processors and installed in the HSMs for securing the processor links.

***Where and with whom are the keys kept?***

Keys are 128 bit random numbers. Operational keys are stored as encrypted data under an MFK (Master File Key) in the HSM. The MFK is normally unknown, and kept on electronic tokens such as IC cards. With internal procedures to meet industry security compliance, keys are kept within the retailers own operations.

***What are the security obligations?***

Retailers who operate HSMs are required to satisfy their processors that they will always keep consumer PIN information secret. This requires compliance with industry standards. Payment Card Industry (PCI) and other standards groups publish security information and audit documents. (See: [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).)

## Implementation

During the implementation phase, Mustang can assist with our knowledge of HSM suppliers, acquiring processors, and other participants. Mustang can also assist in HSM selection. We can provide information about sources, identify alternatives, screen the sales process, and make purchase recommendations.

Mustang can provide a technical interface with acquirers (processors). We can gather information about potential partners, assist in technical interface specification development, gather information about security compliance, and assist in debit transaction testing.

Mustang can assist in HSM startup and production key loading. We can support physical installation of the HSMs, assist with initial (non-secure) testing, assist as needed with Master File Key(s), provide and install the terminal Base Derivation Key (BDK), interface as needed with processors to acquire and install link keys (Zone Keys), and assist with PIN translation issues as production systems go on-line.

## Security Training

The handling of encrypted consumer PINs and the encryption keys that protect PINs require special training and documentation. Mustang understands these requirements and has provided PIN security training to several major retailers and service organizations.

PIN Security training is needed for managers where HSMs are installed and operating, primarily so they understand the seriousness of the responsibility. HSM users and operators need to understand the key hierarchy, and understand the risks associated with all facets of PIN and key security. Application managers and developers need to know the controls required to protect HSMs, to eliminate any opportunity for abuse. Trusted Individuals and Key Custodians need to understand their responsibilities in the safekeeping, transport, and use of keys throughout their life cycle.

Security training and HSM operation requires accurate, complete, and current documentation. Mustang will provide sample documentation, and the industry standards also include many statements that can be incorporated within The Retailers' documentation.

## Security Compliance

Prior to going on-line, The Retailer will have to satisfy the acquirers that PIN encryption keys and operations are secure, as measured by compliance to various standards. Mustang has current knowledge of these standards, and can also act as an independent security reviewer. Once The Retailer has received training and has security documentation, a review of security readiness is performed by an independent person, who can be either an internal auditor or independent person who has current credentials as a reviewer. Mustang has current certification as a PIN Security Reviewer, and can provide this service.

The review includes physical inspection of HSM locations to assure physical and logical (application level) security, inspection of policies and procedures that support PIN security, and inspection of any and all inventory of encryption keys, including records of their protection from the time of creation until the present.

Mustang will gather information about specific requirements for compliance from your selected debit processors, will complete the reviews, and submit the complete packages of compliance documents to the processors. Mustang will submit a statement of compliance based upon the review.

*Questions can be addressed to: Tom Galloway, President, Mustang MicroSystems, Inc., 774-759-9000.*