



## **Facility Requirements for Debit Key Certification**

*January 2005*

Retailers accept ATM (debit) cards at the Point-of-Sale, so PINs must be entered to validate the debit card holder. The PIN is the secret data that allows direct access to consumers' checking accounts, so risk of loss would have a major impact on the acceptance of debit at the POS. The risk is both financial, and also in the loss of consumer confidence if the debit card cannot be used without perceived risk.

When the PIN is entered at an ATM, the electronics are enclosed within a vault, so access to the data is limited. Use of debit cards for retail payment requires the same level of security that surrounds ATM machines, but the PIN is not entered into hardened enclosures as is done in ATMs. Therefore, the security and protection of the consumers' PIN is left to electronic encryption of the data. PINs are protected by the use of secret encryption keys, which are loaded into the PED (PIN entry device). Standards for newer PEDs greatly improve security, but add complexity to key loading process.

Key Injection is done according to several ANSI, VISA, and ISO standards. ANSI has accredited a separate organization ([www.X9.org](http://www.X9.org)), which is responsible for US financial transaction standards, including debit. X9 publishes a Technical Guideline known as the "TG-3", which provides a list of questions for Key Management security reviews.

Standards define an environment and a process to protect the secrecy of keys. Those keys, when loaded into approved "PEDs" (PIN entry devices) protect the movement of consumer PIN data from the retail Point of Sale to the processing networks.

All Keys are protected using the principles of dual control and independent (split) knowledge, using techniques that control access to secret data. Newer procedures also require that "pinpads" be controlled before and after being loaded with secret data. This is done to eliminate unauthorized placement or usage of terminals without proper security so that they might be used to capture PINS for illegal purposes.

### **Approval for Operation**

Companies that wish to do internal key loading must be approved by the partners who share in the transaction delivery from the POS to the issuing bank. The card issuers have the final risk of loss when PINs are compromised. Their only control is to not accept transactions from non-approved service providers, and their main instrument for approval is a completed TG-3 Self Audit, or a similar document such as those offered by Visa, MasterCard, or the ATM networks of Star, Pulse, or NYCE. In order to satisfy the security organizations, an outside audit of the security, facilities, and procedures should be anticipated.

### **Main Components of Key Injection**

When facilities are audited for security, there are three main areas for concern:

#### ***The Encryption Keys***

The heart of PIN security is the initial key exchange and continuous security of the keys – and especially the "human readable" components - during their lifetime. Keys that are loaded into PEDs are shared with the host systems that exchange messages with the terminals.

Since the key transfer ceremonies are relatively infrequent, the procedures need to be well documented and done with the highest security level.

Encryption keys must be kept within a secure room or preferably in separate (dual control) facilities. Records, methods and facilities are required to keep the (human readable) master copies of all keys secure.

### ***The Key Loading Room***

A Secure and dedicated “key injection room” must be constructed. The room requires controlled access, where security encryption keys are injected into target devices. In this room, which is under dual control, will be another (dual control) secure vault for storage of keying material. (Off-Site storage of material for archiving purposes is recommended).

Procedures are required to describe the full operations, access, record keeping, and process in the injection room. Key injection is done by a single workstation (being a PC with no external connections to networks, printers, or modems). The Workstation must use a TRSM to deliver keys to the target PED. (Older key loading tools that use PCs alone are no longer acceptable, since the keys reside in the PC memory). The workstations must not be used for any other purpose.

### ***PED Storage***

Secure storage of all devices that are capable of capturing PINs. By new definitions, this means “from point of manufacture to destruction at End of Life”. Further definition requires storage under dual control (with dual locks and separate key custodians). It also requires accurate records by manufacturer, model and serial number, in a data base that can immediately locate any given serial number and/or account for all units at a specific location. This secure area must be large enough to contain all pinpads that may be present at any one time.

Details of the physical plant, process, and procedures will be reviewed by the approving agencies. The processors may physically visit the key injection facility, and will expect a periodic review.

---

---

Further detail of this information is provided in consulting services available from Mustang. For questions please contact Tom Galloway at the number above.

---

---