Triple DES and Encrypting PIN Pad Technology on Triton ATMs

By: Doug Sholes, Senior Product Manager
Triton Systems of Delaware, Inc.
522 East Railroad Street
Long Beach, Mississippi 39560 USA

November 2002

Where Money Comes From.™

PURPOSE

The purpose of this document is to review the Triple DES encryption specification and Encrypting PIN Pad Technology as it applies to ATMs.

TRIPLE DES NETWORK MANDATE

The national network, MasterCard®, issued a mandate that requires the use of a new PIN encryption algorithm called Triple DES. According to the mandate, "effective April 1, 2002, all newly-installed ATMs, including replacements, must be Triple DES compliant." Later, MasterCard issued a clarification and replaced the word "compliant" with the word "capable." Under the revised term, after April 1, 2002 all newly installed or replacement ATMs must have sufficient hardware and memory to enable Triple DES processing through a software upgrade. By April 1, 2005, all ATMs, including existing terminals, must perform Triple DES. Other networks are expected to follow suit and issue similar encryption mandates.

According to the MasterCard bulletin, "Failure to abide by the triple DES implementation rules could result in substantial monetary penalties that escalate with each repeated violation. Further, noncompliance with the rules ultimately could lead to termination of participation in the MasterCard ATM Network."

TRITON'S RESPONSE

New Triton terminals shipped after April 2002 are fully compliant with the MasterCard Triple DES mandate. Installed terminals with the exception of the 9500 series, the Scrip 9000 and the model 9615, can be made compliant through a Triple DES Upgrade Kit.

ENCRYPTION OVERVIEW

ATM transactions are secured through the use of a PIN (Personal Identification Number), which verifies the identity of the cardholder. Only the cardholder and the card issuer's computer system know the PIN. Encryption is used to protect the PIN by scrambling it and making it unreadable, should a third party intercept the transaction as it travels through the network.

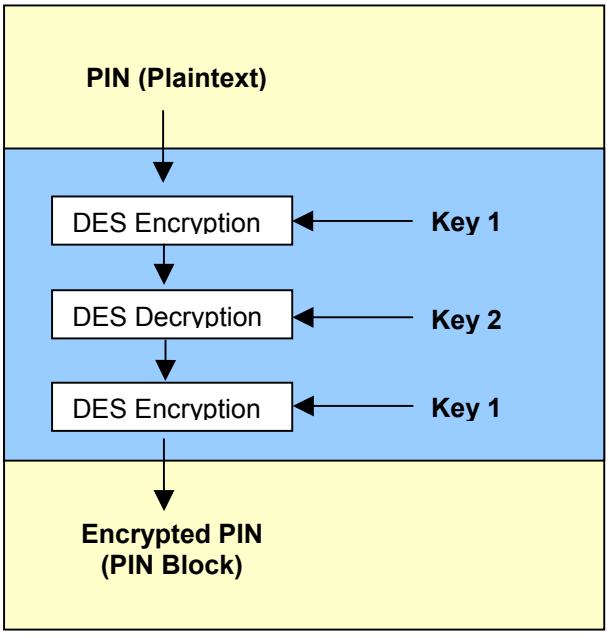
The encryption method that has been a national standard since 1977 is DES (Data Encryption Standard) as described in ANSI X9.8. DES uses a single secret key to encrypt the PIN at the ATM and the same key to decrypt the PIN after it is received by the processor, to verify the cardholder's identity.

The strength of DES has been called into question because of the limited size of its key (64 bits). In 1998 a group called the Electronic Freedom Foundation, using a specially developed computer called the DES Cracker, managed to break DES in less than 3 days. As general technology increases, so does the security required for ATM transactions. Triple DES technology offers a significantly higher level of security. Since it is based on the same algorithm as single DES, it can be introduced into the existing Electronic Funds Transfer (EFT) network with a minimum of disruption. The implementation of Triple DES is necessary in order to maintain public trust in payment systems and to ensure the integrity of confidential cardholder information.

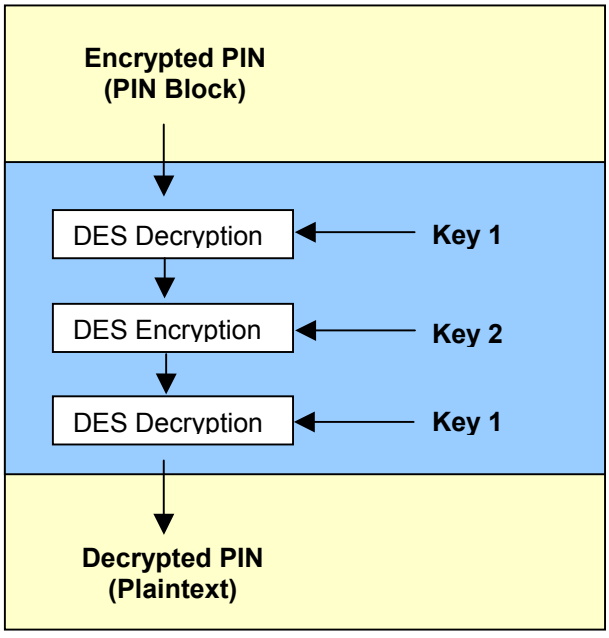
A new specification, ANSI X9.52, was developed to use two 64-bit keys (effectively 128 bits) and apply them three times, hence the name "Triple DES." The procedure for encryption is exactly the same as single DES, but it is repeated three times. Using Triple DES, the PIN is encrypted with the first key, decrypted with the second key and finally encrypted again with the first key.

When the processor receives a transaction generated by an ATM, the procedure for decrypting the PIN is the same, except it is done in reverse.

Encryption within the ATM (EPP)



Decryption at the Processor



ENCRYPTING PIN PADS (EPP) OVERVIEW

In the past, Triton, like all ATM manufacturers, supplied the Tamper Resistant Security Module (TRSM) and keyboard as separate items for terminal shipments within the United States. Combining both features into a single encryption module, an Encrypting PIN PAD (EPP), reduces the opportunity for fraud by encrypting the PIN number before it leaves the terminal keypad. The EPP contains the security processor, the software function, the encryption keys and memory to locally perform the PIN-encryption function. Any attempt to gain access to the EPP will destroy the encryption keys; resulting in failure of all subsequent ATM transactions, until the EPP is replaced and a new set of keys are installed. Using a cryptographic algorithm, the EPP performs a variety of operations, including DES (Data Encryption Standard), Triple DES and MAC (Message Authentication Code). In order to comply with the mandate, Triton requires the use of a Triple DES capable EPP to perform "hardware based encryption."

NEW TERMINAL SHIPMENTS

Every Triton ATM manufactured after April, 2002 is equipped with a Triple DES capable EPP. Software to support Triple DES is available for Triton terminals with the exception of the 9500 family, Scrip 9000 and the 9615. The encryption mode under which the terminal operates (DES or Triple DES) is under the control of the processor. MasterCard expects all processors to process Triple DES transactions for newly installed or reinstalled ATMs by April 1, 2003. Triton ATMs ship with the default encryption mode set to single DES. When the host processor is prepared to support Triple DES, they can enable the feature at the terminal through response messages sent during transactions or through a separate download function.

EXISTING TERMINAL UPGRADES

Existing terminals can be retrofitted with a Triple DES upgrade kit that includes Encrypting PIN Pad and Triple DES software to bring them in compliance with the mandate. All existing models can be upgraded with the exception of the 9500 series, the Scrip 9000 and the model 9615.

The cost of an upgrade on a Triton ATM is a fraction of the upgrade cost for a traditional leased-line ATM. Contact your Triton sales representative for a price quote or visit the Triton WEB site at www.tritonatm.com for more information.

Determining if an existing Triton ATM hardware and software is Triple DES compliment can be done through the ATM Management Functions by selecting the

option "Test Receipt Printer." The printout will list the version number for the EPP keypad (if installed) and terminal software. The Triton Technical Services Department will make the correct determination based on the revision levels of the previously mentioned items.

Triple DES software is backwards compatible in that it will operate in terminals that are not equipped with an EPP or with an older EPP that is not Triple DES capable. In situations where there is a question as to whether an existing ATM is equipped with an EPP that will support Triple DES, the status is determined and optionally reported to the processor through software. Triton Triple DES capable software utilizes the following logic for determining the encryption mode:

Based on the software query diagram, the ATM will notify the processor of one of four possible statuses:

1. Not triple DES capable (no EPP present), default to single DES mode.
2. Not triple DES capable (EPP present, but not triple DES capable), default to single DES mode.
3. Triple DES capable and EPP present, but running in single DES mode.
4. Triple DES capable & operating in Triple DES mode.

If the query results in status numbers one or two, the terminal can be upgraded with a Triple DES Upgrade Kit to enable Triple DES. If the query results in status number three, the processor can enable Triple DES through transaction response messages or through a comms key download.

ATM Software Logic