



**Mustang**  
MicroSystems, Inc.

104 South Street  
Hopkinton, MA 01748  
P: 774•759•9000 F: 774•759•9035  
[www.mustang2000.com](http://www.mustang2000.com)

February 15, 2008

## ***A Managers' Look at Triple DES in Retail Systems***

This paper is a summary description of retail debit PIN encryption as it is being used in early 2008. It is intended for those who are familiar with PIN encryption as it is applied to retail terminals, and may be interested in the conversion now under way – to TDES (Triple DES) DUKPT.

All links between processors and all ATM networks are now using TDES, and recent announcements from the card Issuers (Visa, MasterCard and others) make it mandatory that by July, 2010, all PIN-based debit transactions that originate at retail POS use the TDES method.

Also in 2007, it was announced that as of January 1, 2008 no payment terminal that can be used for PIN-based debit payment can be sold that does not meet the PCI-PED technical requirements for security, and that specification requires TDES capability.

Over ten years ago, a new method of encryption was introduced – called “DUKPT”. It was still based on the DEA (64 bit Data Encryption Algorithm) but used a process that derived and loaded a different Initial Key into each PED (Pin Entry Device), and in turn the PED derived a different key for each transmission, based on the PED’s Initial Key. DUKPT also used a double-wide (128 bit) base derivation key (BDK), which strengthened the process. However, PINs were still encrypted with a single length key.

Over five years ago, security standards groups determined that a technique called Triple DES could extend the useful life of DES. Basically, one half of a double wide key would be used to encrypt the PIN block, and the second key would be used to decrypt it. The result of those operations would again be encrypted by the first key and sent to the host in that form. This TDES method has been used on high volume links between financial institutions for years. This PIN process is well defined in the recently updated ANSI document X9.24 – 2002, and the details of Triple DES are described in ANSI X9.52. Both are available at the [www.x9.org](http://www.x9.org) store.

A combination of DUKPT and TDES, called TDES DUKPT is now being mandated for use in PEDs. DUKPT allows a double-wide Base Derivation Key (BDK) to be used as the source of all keys. A non-reversible encryption process is used to derive from the BDK an Initial KEY (IKEY) for each PED. The biggest difference in TDES DUKPT is in the loading of Initial Keys into PEDs, and the use of TDES within the PED. The original DUKPT used a double length BDK, but only a single width Initial Key was installed in the PED. With TDES DUKPT, a double wide key is installed in every PED. That means that only PEDs capable of receiving and using double wide Initial Keys (and using TDES to encrypt the Pin Block) are compliant with the new TDES DUKPT standard, and this also means that the TDES upgrade will require that the pinpad be directly connected to a secure key loader, either in the field or service depot.

As a registered ESO (Encryption Service Organization), Mustang MicroSystems, Inc. has the system engineering knowledge and facilities to assist any retailer with the conversion to TDES. Our technical staff can help the retailer with understanding the process, creating new keys, testing with the processor, and implementing the conversion.

We would be happy to discuss this technology with retailers who are required to implement TDES.

Please contact our Sales Department for more information.