

Migrating From a Single DES Key to a Triple DES Key in a Triple DES-Capable Terminal

Jeremy King, Business Leader, Global Product and Information Security
Sue Thompson, Product Leader, Global Product and Information Security

Applies to: ✓ Acquirers ✓ Processors

Summary: MasterCard is providing guidance about how merchants and acquirers should migrate from a Single Data Encryption Standard (Single DES) key to a Triple DES key in a Triple DES capable point-of-interaction (POI) terminal.

Action Indicator: **A** Attention warranted

Effective Date: Immediately

Background

MasterCard is currently supporting merchants and terminal manufacturers in the migration of their POI terminals toward Triple DES and Payment Card Industry (PCI) compliance.

Currently, all POI terminals must meet PCI Standards for POS PIN entry device (PED) and Encrypting PIN pads (EPP) compliance mandated by MasterCard. In addition, MasterCard strongly recommends the use of Triple DES for PIN encryption in POI terminals. However, many merchants have continued to use Single DES keys in their pre-PCI terminals. These merchants are now seeking to migrate to Triple DES. This article provides guidance on how merchants and acquirers can undertake the migration of a terminal from Single DES to Triple DES.

Migrating to a Triple DES Key in a Triple DES-Capable Terminal

MasterCard strongly recommends that merchants and acquirers migrate all currently deployed, pre-PCI POI terminals, which use Single DES, to PCI approved, Triple DES compliant POI terminals. While this migration occurs, MasterCard will accept the use of pre-PCI approved, Triple DES compliant, POI terminals.

A pre-PCI approved POS PED or EPP device that uses Single DES can be made Triple DES-compliant based upon the following:

1. The device **must be** Triple DES-capable.
2. If the device is not Triple DES-capable, then the only option available is to replace it with a PCI approved device.
3. The process of injecting a Triple DES key must be undertaken in compliance with the *Payment Card Industry PIN Security Requirements*.
4. The injection of the Triple DES key must be undertaken at a key injection facility that complies with the requirements in Appendix B of the *Payment Card Industry PIN Security Requirements*.

Supporting Documents

The *Payment Card Industry PIN Security Requirements* document, as well as the new *Issuer PIN Security Policy and Guidelines*, can be found on MasterCard OnLine® in the Member Publications product. To view the documents, follow these steps:

1. Navigate to **www.mastercardonline.com**.
2. Log on using your **User ID** and **Security Information**.
3. From the **Products** menu, click **My Products**, then select **Member Publicarions**.
4. From the **Manuals by Category** menu, select **Security/Risk Svcs**, then select **PIN, Terminal, and Wireless Security**.
5. Next select **PIN Security**, and then select the desired document.

For More Information

For more information about the new *Issuer PIN Security Policy and Guidelines* manual or the revised Standards, please contact:

Sue Thompson
Product Leader, Global Product and Information Security

Phone: 44-0-1925-882216

E-mail: sue_thompson@mastercard.com

For more information regarding PCI POS PED and other POI issues, please contact:

Jeremy King
Business Leader, Global Product and Information Security

Phone: 44-0-1925-882212

E-mail: jeremy_king@mastercard.com