Fact Sheet

MasterCard International

MasterCard and Triple DES: Robust Encryption for Greater Protection

MasterCard International is committed to protecting the financial data of its member banks, merchants and cardholders. To help achieve this, MasterCard is working with its partners to upgrade to the strongest existing encryption standard, Triple DES, for ATMs and point-of-sale devices.

How Encryption Works

Encryption protects sensitive data from intrusion. It uses a set of rules (algorithm) and an additional piece of data (key) to transform readable data (plain or clear text) into an unreadable, scrambled form (cipher text). The recipient of the cipher text uses an algorithm and a key to apply an inverse transformation (decryption) to be able to read the clear text.

DES Background

In 1974, the Data Encryption Standard (DES) was developed and then adopted in 1977 as a national security standard to protect electronic information. However, in 1998, the Electronic Frontier Foundation demonstrated that it is possible to crack DES, thus calling for an upgraded security standard to defend the financial services industry. The result was the development of Triple DES – a much more secure standard – which has become central to the protection of today's financial data. Triple DES uses the same algorithm as DES but invokes that algorithm three times in a single encryption request instead of just once. The result of this process is data that is exponentially more secure during transmission than data protected with "single DES."

MasterCard and Triple DES

MasterCard International staff began working closely with members, vendors and processors in 1999 to migrate personal identification number (PIN) processing, including ATM and point-of-sale processing to Triple DES, using a double-length (16 byte, 112-bit) or triple-length (24 byte, 168-bit) key for online transactions.

In 2000, MasterCard, Maestro, and Cirrus adopted Triple DES as the standard requirement for host processing systems and terminals to help ensure the integrity of the payment system. MasterCard is assisting its members with the assessment and testing of their software and systems so that they can implement Triple DES. Total Triple DES processing will be achieved using a phased implementation approach for ATMs and other POS devices through the point of authorization.

MasterCard's Calendar for Total Triple DES Compliance

MasterCard has mandated that financial institutions and merchants ensure that all ATMs and newly installed merchant point-of-sale terminals be Triple DES compliant.

Two of the three major Triple DES compliance milestones have already been passed:

- MasterCard mandated that all newly installed merchant terminals and ATMs were to be Triple DES capable as of **April 1, 2002**.

- As of **April 1, 2003**, all host systems (links) had to be Triple DES compliant.

By **April 1, 2005**, all ATMs must be Triple DES compliant. MasterCard also is ensuring that its chip and e-commerce programs are Triple DES compliant. PIN-entry point-of-sale devices must meet Triple DES criteria. A sunset date for existing devices will be announced soon.

###

Updated August 2004