



What is PCI & Triple DES?

Overview

Payment Card Industry Data Security Standard (PCI DSS) was created to protect sensitive customer data through a unified set of data security measures and reduce debit card fraud. It accomplishes this by:

- Setting standards for handling transaction data
- Governing the encryption of Personal Identification Numbers (PIN)

Debit customers enter PIN on keypads at both indoor and outdoor terminals, including CRIND™ Card Reader in the Dispenser.

Triple DES

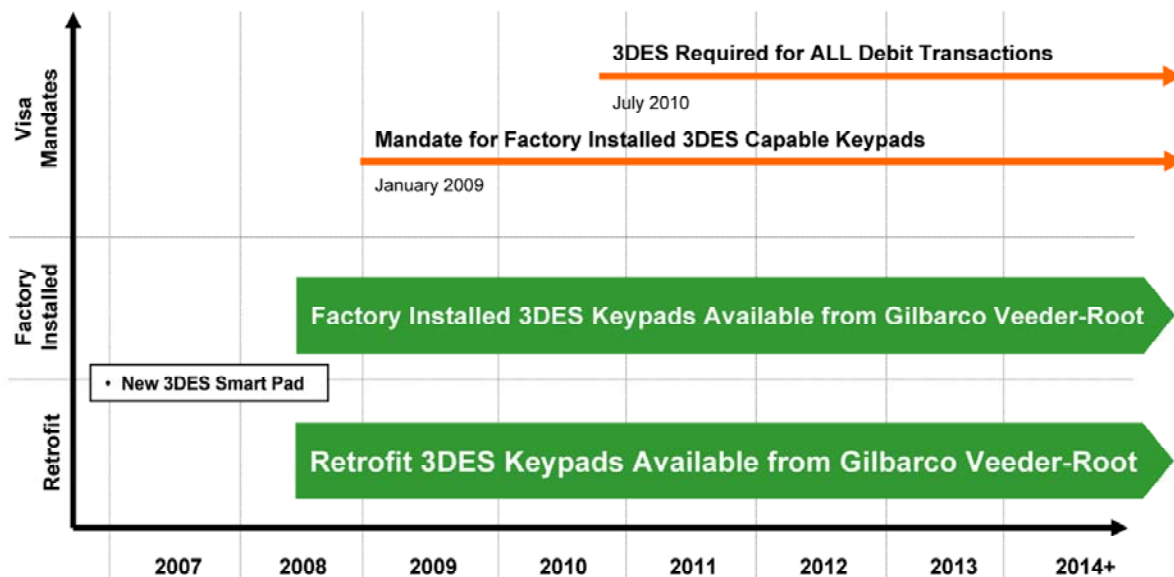
Triple Data Encryption Standard (3DES) is the mandated method of securely protecting customer PIN information during debit transactions. This method involves encrypting the information multiple times in the keypad, using an Encrypted PIN Pad (EPP). Retailers processing debit transactions must comply with the mandated timeline for all dispenser hardware and infrastructure in the US region to use an EPP processing 3DES format.

Who sets the compliance mandates?

PCI Security Standards Council is an organization founded by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. While PCI establishes a common set of standards that many card associations subscribe to, each individual card association defines its own mandate compliance dates.

What is the timing for implementing Triple DES?

US Triple DES Timetable (3DES)



Gilbarco Veeder-Root Product Offering

PCI EPP approved 3DES capable FlexPay™ Encrypting PIN Pad for the U.S. market.

- Compatible with existing payment infrastructure and POS systems.
- Compatible with all Gilbarco® dispenser configurations and options.
- Backward-compatible feature available if your payment network is not ready for 3DES Derived Unique Key Per Transaction (DUKPT).
- Factory-installed option for Encore® S and Encore 300. Retrofit kits are available for all post-modular Gilbarco dispensers.

