MAGTEK®
SECURITY FROM THE INSIDE

PA-DSS STATEMENT FOR PAYMENT APPLICATIONS

In September of 2010, Troy Leach, the Chief Standards Architect for PCI DSS, stated; "properly implemented P2PE will allow merchants to reduce their scope in complying with the Payment Card Industry Data Security Standard. This is a significant statement; the PCI Council has never made this statement before."

Based on this statement as well as other published statements, opinions, and input gained from the certification of our own hardware products and Magnesa.net's Services, MagTek is confident in stating that the use of MagTek's MagneSafe™ Security Architecture (MSA), in combination with our certified Magensa.net Payment Protection Gateway, may allow customers employing these systems together to reduce or entirely remove their application from the scope of PA-DSS compliance.

By encrypting the card data at the earliest possible point (inside the read head and at the moment of swipe), using an industry standard encryption method (3DES), dynamic encryption keys (DUKPT), and not providing the encryption key to the application vendor, MagTek and Magensa.net are following the best practices accepted in the industry regarding Point to Point Encryption.

MagTek and Magensa.net go beyond this level of encryption security however, by providing token services, and card authentication services (MagnePrint®) based on dynamic payment card data. This additional protection is important and valuable based on the comments of Bob Russo, General Manager of PCI DSS, who stated; "We believe the PCI Security Standards provide a solid foundation for a security strategy to look after your payment and other types of data, but security does not start and end with compliance. Focus on good security and compliance will follow." It has always been part of MagTek's mission to lead the way in terms of card data security and by providing additional card security features now; the MagneSafe Security Architecture can help future proof your application in an ever-changing environment.

Software developers that do not want to go through PA-DSS should exclude the collection of Payment data in their applications. Instead, they should use Secure Card Reader Authenticators (SCRAs) and a virtual terminal like that provided by Magensa.net to collect and process cardholder data. If their application collects cardholder data, even if encrypted, according to PCI they must comply with PA-DSS.

It should be noted: ***The primary account number (PAN) is the defining factor in the applicability of PCI DSS requirements and PA-DSS***. PCI DSS requirements are applicable if a primary account number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed, or transmitted, PCI DSS and PA-DSS do not apply." This language is straight from the Payment Card Industry (PCI) Payment Application Data Security Standard, Requirements and Security Assessment Procedures, Version 2.0, dated October 2010. Hence, an application that does not collect a PAN can be entirely removed from the scope of PCI PA-DSS.

An application that does process cardholder data, while in scope for PA-DSS, can still see significant reduction in the scope of its certification process by the use of MagTek SCRA's and the Magnesa.net Payment Protection Gateway

The requirements of PA-DSS are listed below.

1. Do not retain full magnetic stripe, card verification code or value (CAV2, CID, CVC2, CVV2), or PIN block data
2. Protect stored cardholder data
3. Provide secure authentication features
4. Log payment application activity
5. Develop secure payment applications
6. Protect wireless transmissions
7. Test payment applications to address vulnerabilities
8. Facilitate secure network implementation
9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote access to payment application
11. Encrypt sensitive traffic over public networks
12. Encrypt all non-console administrative access
13. Maintain instructional documentation and training programs for customers, resellers, and integrators

The use of MagTek SCRAs and the Magensa.net Payment Protection Gateway, when properly implemented, will dramatically reduce the scope of Requirements 1, 2 and 11 and provide additional scope reduction for requirements 3, 5, 6, 7, 9, 10, and 12.

In order to take advantage of the reduced or eliminated PA-DSS scope that may be achieved by the combination of MagneSafe equipped SCRAs and the Magensa.net Payment Protection Gateway, the following conditions must also exist.

1. All card reading must be accomplished by the use of MagneSafe-enabled secure card reader authenticators (SCRAs).
2. No manually, keyed entered transactions are permitted through any application interfaces. Key entered PANs for card not present transactions must be entered on a MagTek (PCI PED2.x certified) IPAD®.
3. All transactions must be routed through the Magensa.net Payment Protection Gateway.
4. Neither the merchant nor the application provider possess or have access to the decryption keys used by the SCRAs to encrypt the cardholder data.
5. The SCRAs are set to Security level 3 or above.

As with all Payment Applications, the final determination of applicability of PA-DSS should be performed by a qualified PA-QSA.