MAGENSA™
A MAGTEK COMPANY

Designing a POS system for cost-effective compliance with PCI-DSS:

Using MagTek readers and Magensa processing services

White paper

Magensa, LLC, 1710 Apollo Court, Seal Beach, CA 90740 | p 562-546-6400 | f 562-546-6301 | www.magensa.net

1 Executive Summary

The potential for an unauthorized release of cardholder data is a critical concern for any of the players involved in the business of acquiring and processing card-based payments. This includes merchants, service providers, gateways and processors. It also includes, by proxy, entities that provide software and solutions to merchants, even though they themselves may not be involved in processing transactions. This includes ISOs, ISVs, VARs and software developers. Data breaches expose all these parties to the risk of financial loss in the form of litigation, as well as penalties leveled by card brands and regulatory agencies.

Therefore, the mitigation of this risk is an essential element in any POS system design. The question, however, is *how* this is best accomplished. Given the sophisticated nature of many of the methods available to protect cardholder data, choosing the correct path can be daunting. The decision is made even more difficult by the imposition of requirements for cardholder data protection by the PCI Security Standards Council, often referred to simply as "PCI". This organization promulgates the PCI Data Security Standard, PCI-DSS, a standard by which virtually all members of the card acquiring chain must adhere (either directly, or on behalf of their customers).

So, a difficult task becomes two: Protect cardholder data, and thus the organization, from a data breach *and* show that the requirements of PCI-DSS have been met. Since investments in risk mitigation do not generally contribute to revenue, most organizations scramble to limit the scope of cardholder data protection to as simple and cost-effective a solution as possible. This is only rational. It is important to remember that payment card crime is a cost/benefit game: The amount spent on securing cardholder data should be *l*ess than the expected losses over time. This is also reflected in a criminal's analysis of the profitability of stealing card data: If it costs more to steal it than it's worth, it's avoided.

2 Security Methodology

Given these guard rails, how should one navigate the road? We recommend choosing a security methodology for your design that accomplishes all these needs *at once*. Only one such methodology has proven itself time and again, across billions of transactions, to be the best choice and is accepted by PCI: ***Completely remove all unencrypted cardholder data from your environment by insuring that it is strongly encrypted by a responsible third party, with a key only they know, before it reaches your environment and stays that way until it leaves.*** With MagTek encrypting readers and Magensa gateway processing, you can achieve this goal.

We suggest this methodology as it is at the heart of effective PCI-DSS compliance. At its core, PCI-DSS is about protecting cardholder data, specifically the card number or Primary Account Number (PAN). From the PCI-DSS standard[1]:

> "The primary account number is the defining factor for cardholder data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), they must be protected in accordance with applicable PCI DSS requirements."

[1] PCI Security Standards Council, "Data Security Standard, Requirements and Security Assessment Procedures", *www.pcisecuritystandards.org*, Version 3.2, April 2016, p. 7.

This raises a question. If you only have access to cardholder data that is strongly encrypted with keys you do not have access to, do you really have a CDE? The answer is still yes, but with an important caveat.

From PCI FAQ 1086[2]:

> "Where a third party receives and/or stores only data encrypted by another entity, and where they do not have the ability to decrypt the data, the third party may be able to consider the encrypted data out of scope if certain conditions are met. For further guidance, refer to FAQ 1233: How does encrypted cardholder data impact PCI DSS scope for third-party service providers?"

From PCI FAQ 1233[3]:

> "Where encrypted cardholder data is shared with a third party, responsibility for the data generally remains with the entity or entities with the ability to decrypt the data or impact the security of the encrypted data."

Additionally:

> "As another example, a third party that receives only encrypted cardholder data for the purposes of routing to other entities, and that does not have access to the cardholder data or cryptographic keys, may not have any PCI DSS responsibility for that encrypted data."

In both cases, the third-party (the merchant, gateway or service provider), receives data from a MagTek reader already encrypted with a key it does not know, and sends it, still encrypted, to Magensa for final processing to a merchant processor or other endpoint. In essence, these organizations are depending on MagTek and Magensa's compliance with PCI-DSS (Level 1), substituting it for their own. They have practiced *segmentation*, as defined by PCI, for removing cardholder data from their environment.

This is at the heart of a concept that is often mentioned in relation to PCI: "scope reduction". Scope refers to the degree and extent to which an organization's software and systems must be *demonstrated* to be in compliance with PCI. In general, the greater the scope, the greater the cost of demonstrating compliance. The use of encryption as described above greatly reduces that scope.

But even with the scope greatly reduced, compliance with PCI must still be demonstrated. Though the cardholder data is encrypted, it is still there. But how compliance is shown (and to whom), greatly affects cost. There is a great deal of misunderstanding in the industry on this point, so careful understanding is important.

First, know to whom compliance must ultimately be shown:

- It is *not* PCI. PCI promulgates cardholder data security requirements through documents they term "standards". PCI itself does not audit organizations or evaluate solutions. From the PCI website[4]:

[2] PCI Security Standards Council, "PCI FAQ 1086", *www.pcisecuritystandards.org/faqs*, December 16, 2019
[3] PCI Security Standards Council, "PCI FAQ 1233", *pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/How-does-encrypted-cardholder-data-impact-PCI-DSS-scope-for-third-party-service-providers*, December 16, 2019
[4] PCI Security Standards Council, *www.pcisecuritystandards.org/about_us/*, December 16, 2019

    - "Enforcement of compliance with the PCI DSS and determination of any non-compliance penalties is not part of the Council's scope of activities. Any questions in those areas should be directed to the payment brands or the entity responsible for payment processing."
- It is *not* PCI auditors, at least not directly. PCI auditors, or Qualified Security Assessors (QSAs), are third parties that evaluate your compliance with PCI-DSS, at your cost. Such an evaluation is their *opinion* of your compliance. It can be accepted or rejected by those entities that must be shown compliance:
- The Payment Card Brands.
    - Ultimately, these organization decide whether to accept a payment card transaction from a system or not, based in part on its level of security. The payment card brands generally base this decision on compliance with PCI, *as they see it*. For nearly all members of the acquiring chain, PCI compliance is demonstrated to the payment card brands through organizations that act as their proxies for this purpose: *the merchant processors*.
    - They also assess penalties if an organization is involved in a data breach. The assessment of said penalties depends only on the breach – the fact that an organization may have been deemed PCI-DSS compliant at some point in the past is irrelevant.

3 Demonstrating Compliance

With this in mind, how then does an entity demonstrate compliance with PCI-DSS? First, remember that only those entities handling cardholder data are assessed. Software and solution providers that do not themselves handle cardholder data are not included, though their merchant customers *are*. Therefore, these entities should be prepared to assist their customers in meeting their PCI-DSS compliance requirements. Second, demonstrating compliance (rather than compliance itself) has its own standards, promulgated again by PCI and accepted by the payment card brands. They are composed of a hierarchy of *compliance levels* that are used to categorize an entity and determine which assessment methodology is required. For our purposes, only two levels are important[5]:

- Level 1. Organizations processing more than six (6) million transactions per year. These organizations must undertake an onsite audit performed by a QSA hired by the organization and have a Report on Compliance (ROC) produced.
- All entities processing less than Level 1. Complete a self-assessment questionnaire (SAQ), a series of questions answered by the entity itself. Returning to our idea of cost-effectiveness, we can now see that if an organization is not Level 1, *it does not need an onsite audit.* Preparing a SAQ is far simpler and less expensive.

Now that the assessment method has been determined, how is it completed as cost-effectively as possible?

1. PCI Level 1 audit – The QSA should be provided the following information:
    a. All card data (EMV and MSR) is encrypted by MagTek readers using TDEA encryption and DUKPT dynamic key management (both per ANSI X9) before reaching any system

[5] Other levels may have additional, ongoing test requirements, such as network scans.

or software in the organization. This is true for all MagTek readers, whether PCI PTS certified or not.

b. The organization certifies it is not in possession of, nor has access to, the DUKPT BDK, therefore is unable to decrypt the reader data itself.
c. Payment card transactions are processed with the encrypted reader data directly to Magensa, a PCI Level 1 gateway.
d. There are no other connections to cardholder data other than that provided by MagTek readers. This includes manually entered card data. If such data exists, the QSA must audit the systems that process them. MagTek has additional solutions for encrypting (and more importantly, *securing*) manually entered cardholder data that are useful in these situations.

2. SAQ, version D (there are other SAQs, but they are not applicable to this discussion). The organization can obtain a pre-filled copy of the SAQ D from its Magensa sales representative. All assessment questions related to the protection of cardholder data will be answered by Magensa.

4 Final thoughts

Many industry participants, and sadly some QSAs, believe that achieving scope reduction, as outlined in this paper, requires a PCI certification known as "PCI-P2PE". This is not true. In fact, the scope of a PCI assessment is determined by the organization itself. From PCI[6]:

> "Ultimately each entity is responsible for making its own PCI DSS scoping decisions, designing effective segmentation (if used), and ensuring its own PCI DSS compliance and related validation requirements are met."

PCI-P2PE compliance is not required by PCI or any payment card brand to be compliant with PCI-DSS. In fact, the use of a PCI-P2PE compliant solution *does not* guarantee compliance with PCI-DSS. As noted, scope reduction is achieved with strong encryption and segmentation.

In addition, any organization that handles cardholder data, encrypted or not, will be deemed a part of the PCI-P2PE solution if such a certification is desired. This will require the organization to participate in the PCI-P2PE assessment. These are more intensive and difficult than even PCI Level 1 audits. There is no SAQ to become PCI-P2PE compliant.

Fortunately, leading QSAs have recognized the approach to scope reduction defined in this paper. Coalfire, in its PCI-DSS assessment of the leading healthcare payments system provider, InstaMed (now a J.P. Morgan company), determined that the use of MagTek readers and Magensa processing is a powerful way to reduce risk and meet the obligations of PCI-DSS:[7]

> "During this assessment, Coalfire validated that InstaMed adheres to the applicable compliance control requirements for potentially reducing the applicable controls during a merchant's PCI DSS compliance audit."

[6] PCI Security Standards Council, "Guidance for PCI DSS Scoping and Network Segmentation", *www.pcisecuritystandards.org,* Version 1.1, May 2017, p. 4.
[7] Coalfire, "Security & Encryption in Healthcare Payments, PCI DSS Technical Assessment", *www.instamed.com*, p.15