P2P Encryption

REDUCE PCI SCOPE, PROTECT CARDHOLDER DATA AND PRESERVE PROFIT

For merchants and their providers that have addressed the hurdles of achieving and subsequently maintaining PCI compliance by relying upon segmentation of their payment network, the fight to protect cardholder data never ends. It is a daily uphill battle that becomes resource exhausting over time. There are many important lessons that can be learned by understanding the challenges of this battle as it is currently being fought – lessons that can ultimately lead to a more effective means of protecting cardholder data.
Our purpose is to arm merchants and integrated business management software providers (ISVs) with the knowledge and tools to address the following targets all in the spirit of preserving brand and profit.

- **Eliminate Cardholder Data**
- **Reduce PCI (PCI DSS and PA DSS) Scope**
- **Reduce PCI Costs**
- **Enable Operational Efficiency Within Business Management Applications**
- **Reduce Data Compromise Risk and Liability**

In this document we compare the benefits and pitfalls of reliance on payment network segmentation to the robust option of point-to-point encryption (P2PE) coupled with tokenization in a highly secured hosted environment.

To appreciate the options presented in this document, a Fort Knox analogy is a helpful starting point.

In 1937, the US Treasury Department established the Bullion Depository at Fort Knox to protect highly valuable U.S. gold reserves from thieves. Not only was the structure expensive to build, it was equally expensive and challenging to secure against the constant threat of thieves. The Fort was a centralized target and quite literally a goldmine for thieves who could break through the security established at Fort Knox. Gold has always been and continues to be a target for thieves because it has significant value.

The payment industry is dealing with a similar situation. Merchants segmenting their payment network are building their own expensive fort (or perimeter) to protect their gold – or in this case, cardholder data. Constant cyber threats have forced these same merchants to continuously invest significant funds into maintaining their fort in accordance with the PCI and other security standards. These merchants remain a target for cyber threats, but options now exist that can remove them as a target. If merchants implement a solution that eliminates the gold thieves are after, the costs to build and maintain their highly protected fort would diminish considerably. The proper Point-to-Point Encryption (P2PE) solution can make this vision a reality for merchants by eliminating the cardholder data in their possession, which in turn removes the merchant’s payment network as a target. In doing so, this approach significantly reduces most of the merchant’s PCI burden.

P2PE solutions couldn’t be more welcomed given the current state of cardholder data security. Any merchant who has experienced a compromise firsthand quickly welcomes the surrender of their PCI responsibilities? Headlines loom with story after story of a merchant’s payment environment being compromised by cyber thieves.

In response to these reports, merchants and their providers scramble to find solutions that protect cardholder data. Many of these solutions focus on traditional perimeter security referred to as “network segmentation”. These solutions often attempt to provide more protection for the consumer, although the compromise statistics show differently.

To provide a more effective answer to known security challenges, Element Payment Services, a leading technology solution and payment processing provider, has teamed up with the payment industry to provide a comprehensive P2PE solution, called Element TransForm™. Element’s advanced...
solution provides more security for and efficiency over managing cardholder data than the traditional payment network segmentation model. Specifically, their comprehensive TransForm™ P2PE solution also prevents a merchant from enduring the high PCI DSS cost, risk and liability that exists with the reliance on payment network segmentation. Their solution extends beyond securing cardholder data on behalf of the consumer. It enables merchants to secure their profitability, by significantly reducing risk and liability with a focus on eliminating cardholder data. Through this new approach to protect cardholder data, determining the optimal payment solution for a merchant becomes a function of the merchant’s risk appetite and desire to protect their brand.

Before discussing the benefits of TransForm™ P2PE and the limitations of the traditional network segmentation model, it is important to clarify how we define cardholder data (value) versus non-cardholder data (no value). Understanding this point is the silver bullet to a merchant limiting risk.

**CARDHOLDER DATA VERSUS NON-CARDHOLDER**

What exactly constitutes cardholder data and makes it so valuable to thieves? Knowing the distinction between what is and what is not cardholder data is an important and cost-related point relevant to a merchant’s evaluation of a payment solution.

Cardholder data, as defined by the card brands and PCI Security Standards Council (PCI SSC), includes:

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAN</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td></td>
</tr>
<tr>
<td>Service Code</td>
<td></td>
</tr>
<tr>
<td>Expiration Date</td>
<td></td>
</tr>
</tbody>
</table>

**TABLE 1 CARDHOLDER DATA**

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Magnetic Stripe</td>
<td>No</td>
</tr>
<tr>
<td>CVV2/CVV3/CID</td>
<td></td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td></td>
</tr>
</tbody>
</table>

Where cardholder data exists in a “readable” format the PCI standards will apply to the merchants network. Alternatively, eliminate or render permanently “unreadable” the cardholder data elements and the PCI scope, along with sole reliance on payment network segmentation, can be significantly reduced.

<table>
<thead>
<tr>
<th>Readable (Cardholder Data = Value)</th>
<th>Unreadable (Non-Cardholder Data = No Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full PAN in clear 411648059370132+</td>
<td>PAN fully truncated XXXXXXXXXXXXXXXX+</td>
</tr>
<tr>
<td>PAN partially truncated less than the first 6 last 4 - 411648XXX0132+ or 411648XXX0132+</td>
<td>PAN Truncated to at least the first 6 and last 4 - 411648XXXXXXX0132+</td>
</tr>
</tbody>
</table>

**TABLE 2 CARDHOLDER DATA (READABLE) VERSUS NON-CARDHOLDER DATA (UNREADABLE) TO POS MERCHANT**

1 Card Data Elements are only considered Cardholder Data when stored in connection with the PAN

2 Table 2 provides specific examples, relevant to this document, of how to devalue cardholder data. Additional information of “readable” and “unreadable” data can be found on the PCI Security Standards Council’s website www.pcisecuritystandards.org
CARDHOLDER DATA DEFINITION
(per the PCI SSC)
Sensitive authentication data or the PAN plus any of the following: cardholder name, expiration date, and service code.

“READABLE”
Unencrypted data element and/or encrypted data with a merchant having access to the de/encryption key or partially truncated PAN.

PERMANENTLY “UNREADABLE”
Encrypted data elements with the merchant having no access to the de/encryption key or truncated PAN.

Table 2, on the previous page, list examples of “readable” data converted to “unreadable” data. Once data is rendered “unreadable” the data is no longer classified as cardholder data. In fact, the PCI SSC clarified this point by stating “encrypted data is out of scope if, and only if, it has been validated that the entity that possesses encrypted cardholder data does not have the means to decrypt it.” Since PCI standards apply only to networks where cardholder data exists, it is logical that the PCI scope is significantly reduced or eliminated where the data was rendered “unreadable.”

Cardholder data in its readable form is like gold – it has value to cyber thieves as they can sell the information for cash or use it to perform criminal activity. Eliminate cardholder data and/or render the data unreadable, and you remove the data’s value rendering it useless to thieves. In doing so, a merchant removes itself from the constant threat and target of cyber thieves.

Let’s briefly review how cardholder data exists and is protected within the traditional payment network segmentation model.

TRADITIONAL CARD DATA PROTECTION MODEL: PAYMENT NETWORK SEGMENTATION

Until recently, security providers advised merchants to protect cardholder data by segmenting their payment systems from other parts of their technology environment using perimeter security controls in an effort to reduce the PCI scope. This is referred to as “payment network segmentation.” Implementing a payment network segmentation design means segmenting a merchant’s payment devices and servers - that handle cardholder data - from all other network components. Other components may include email servers, web servers, databases, etc.

Payment network segmentation serves two purposes: 1) Limit access to cardholder data, and 2) Limit the PCI scope. An example of traditional payment network segmentation for a point-of-sale merchant is illustrated below.

In reference to Diagram 1 below, a segment would include the Internal Network, Protected Network, POS Network, etc. Most segmented network structures include specific hardware, software and maintenance designated for each segment. Specifically for the POS Network segment, the structure must also meet the spirit of the PCI DSS. For instance, each segment often includes a dedicated firewall, dedicated connection/line, and separate access controls combined with the supporting services of file integrity checking, patch management, secure coding, anti-virus checking, audit logging and storage, vulnerability scans, penetration testing (web servers), secured offsite backup, etc. These costs are often redundant with the other network segments within the merchant’s environment. In addition, the merchant must address compliance using the same 200+ questions on the PCI Self-Assessment Questionnaire that they would have had to address under the no-segmentation model. The price tag and duplication of effort adds up quickly if the network structure is not designed and managed appropriately.

DIAGRAM 1

2 PCI SSC Initial Roadmap: Point-to-Point Encryption Technology and PCI DSS Compliance, Article #10359 on the PCI SSC FAQ website
Next to these redundant costs, another downside to network segmentation is that it does not reduce the volume or readability of cardholder data leaving their fort of gold a target for cyber thieves. The same amount of cardholder data exists in the network segmentation model as in its previous no segmentation model, yielding little change to the risk and liability associated with protecting cardholder data. According to the Privacy Rights Clearinghouse, the breach liability for a merchant handling cardholder data is approximately $180 to $1,000 per cardholder number transmitted and stored. Many merchants still store over five years of cardholder data yielding a potential liability of $135,000 to over $600 million USD should their payment network be breached. The annual PCI costs combined with the overall cardholder data transmission and storage liability is unaffordable for most merchants. Based on our experience, the average annual costs to achieve PCI compliance securely transmit cardholder data and store such data ranges from $30,000 to $2.2 million USD.

Although the disadvantages of payment network segmentation can be significant, this approach does have its advantages:

1. Restricts access to cardholder data
2. Limits PCI scope to only the network segments with access to cardholder data
3. Slightly reduces the PCI audit costs (compared to no network segmentation)
4. Spreads the costs of network supporting services across multiple cost centers/divisions

It is recognized that with any payment solution a merchant may need to maintain segmentation of other components within their network to ensure security of those areas and/or for other policy reasons not related to PCI. We recommend merchants quantify and compare the advantages and disadvantages of a network segmentation design with Element’s comprehensive TransForm™ P2PE solution before continuing with the traditional network segmentation model.

**POINT-TO-POINT ENCRYPTION (P2PE)**

P2PE can be defined as a solution that encrypts card data from the entry point of a merchant’s point of sale to a point of secure decryption outside of the merchant’s environment, such as a payment processor, as illustrated in the diagram below. In a P2PE environment cardholder data is not in the clear, and the confidentiality and integrity of the data-in-motion is maintained securely point-to-point.

P2PE is intended to directly address the risk of unauthorized interception associated with cardholder data-in-motion such as during transmission of a transaction from the POS terminal to the payment processor. It does not address data-at-rest (stored cardholder data) in legacy or other systems used for ongoing operations. Tokenization is intended to address the risk of unauthorized access associated with stored cardholder data. The combination of P2PE and tokenization creates a comprehensive and powerful solution for merchant and consumer data protection.

As illustrated below, if a POS terminal or hosted virtual terminal encrypts the cardholder data at swipe and the merchant does not have access to the de/encryption keys, then the data is deemed “unreadable” to the merchant.

---

**Diagram 2**

**P2PE (DATA-IN-MOTION) AND TOKENIZATION (DATA-AT-REST)**

[Diagram showing the flow of encrypted card data from POS terminal to merchant server to payment processor and vault.]
Per the PCI SSC, the PCI standards only apply to the areas of a merchant environment that store, process and/or transmit cardholder data. When a merchant selects the proper hosted encryption solution, the solution encrypts the card data at swipe (for card present payments) or key entry (for card not present payments). The merchant has no access to the keys required to decrypt the data, thereby rendering the data as non-cardholder data (“unreadable”) to the merchant. This means that a merchant’s PCI-related scope and costs are reduced incrementally. Specifically, the PCI dSS requirements are reduced to only 1, 9 and 12 being directly applicable to the merchant’s environment. To learn more about the 12 PCI DSS requirements visit: www.elementps.com/merchants/pci-dss-requirements.

When evaluating P2PE solutions, a merchant can maximize their benefit by ensuring the selected P2PE solution operates complimentary to the following Payment Solution Selection Criteria.

### PAYMENT SOLUTION SELECTION CRITERIA

#### Hosted Solution “Software-as-a-Service” or “SaaS”

In order for a merchant to reduce their PCI scope, costs and liability - without giving up card acceptance - the merchant must shift the responsibility to a secured payment hosting provider. The hosted provider handles transmission, processing and storage of cardholder data on behalf of the merchant. The merchant’s servers and databases are freed from resource-intensive card transmission, storage and encryption functions. This can significantly streamline technology resources within the merchant’s environment.

For business management application providers (ISVs), a hosted solution removes the burden of PA-DSS validation associated with an ISV’s application distributed for merchants use in their payment environment. For ISV’s offering a SaaS solution, integration of their application with a secured payment hosting provider removes the burden of PCI DSS and card brand registration requirements by shifting such responsibilities to the hosted processing provider.

#### Hosted Tokenization

Merchants that need certain payment transaction details stored in their internal legacy systems to assist customers can still do so when they select a solution that provides tokenized data. For example, merchants may need payment data to manage customer dispute resolution, recurring/subscription payments, card-on-file billing and targeted marketing and analytics. “Tokenization substitutes unique, randomly generated values to reference cardholder data that are typically stored in the merchant’s facility (or offsite), eliminating the need for merchants to store and protect actual cardholder data.”

When a secured hosted P2PE solution is implemented with a tokenization method it makes it virtually impossible for a cyber-thief to compromise access to both the token and valuable data.

#### ISV Fully Integrated Solution

Optimally, if a merchant uses a software solution to manage their business operations they should ensure the hosted solution is compatible with the software. This allows automatic posting of product/service sales between the hosted payment module and the operations/finance module, eliminating manual entry and tracking of activity between two unconnected sources. It is also important to ensure a seamless experience for the merchant’s customers between the merchant website and the payment screen.

---

4 Aberdeen Group, “Avoiding a Kick to the Head: The Value of Tokenization for Protecting Cardholder Data” (Feb. 2010)
Device Interoperability

Legacy POS devices often were not equipped by vendors to perform encryption at swipe or entry. When implementing a P2PE solution, merchants need to ensure that their POS device accepts the selected encryption solution. Often this requires installing a new POS device or software to ensure device compatibility and driver installation unless the merchants can select a driverless solution. Merchants should also look for P2PE providers that are device agnostic and offer solutions appropriate for the payment environment.

Diagram 3, on the right, illustrates the payment network solutions available to merchants today and how a solution which incorporates the Payment Solution Selection Criteria above impacts the level of PCI costs/scope, risks and liability.

When comparing the available non-hosted (merchant managed) solutions to the hosted solution, it becomes clear that the hosted solution is the optimal solution to control PCI costs, scope, risk and liability. Only by no longer accepting card payments can a merchant so completely control PCI costs, scope, risk and liability – an unreasonable option that would limit a merchant’s profitability and service offering.

Table 3, on the left, can be used to assist merchants with their comparative return on investment calculation when evaluating their existing payment network costs and liability to a hosted P2PE with tokenization approach.
Further, our research of 32 merchants between 2008 and 2011 indicated that the PCI cost reductions almost directly correlate to the number of requirements applicable to the merchant’s implemented solution as indicated in the chart below.

### Table 4: Merchant Approach: Impact to PCI Scope

<table>
<thead>
<tr>
<th>Merchant Approach</th>
<th>PCI DSS SAQ Version</th>
<th>Merchant Applicable # of Steps</th>
<th>Merchant PCI Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor/gateway hosted, P2PE and tokenization (CNP only)</td>
<td>A</td>
<td>6</td>
<td>Very limited</td>
</tr>
<tr>
<td>Processor/gateway hosted, P2PE and tokenization</td>
<td>C</td>
<td>6</td>
<td>Very limited</td>
</tr>
<tr>
<td>ISV hosted and merchant cardholder data access, no card data storage</td>
<td>C</td>
<td>19+</td>
<td>Limited</td>
</tr>
<tr>
<td>Network segmentation (not hosted)</td>
<td>D</td>
<td>&lt;220</td>
<td>Slightly reduced</td>
</tr>
</tbody>
</table>

Selecting a comprehensive, secure P2PE solution provides a merchant benefits that far exceed that of reliance on network segmentation. With a P2PE solution, the merchant:

1. Eliminates cardholder data
2. Reduces PCI DSS scope from 220 to 6 PCI steps
3. Significantly reduces PCI costs in alignment with PCI scope reduction
4. Enables operational efficiency within ISVs applications
5. Data compromise risk and liability becomes negligible

As with any solution, a merchant will need to maintain certain controls in order to ensure maximum security of any payment environment, such as:

1. Conduct annual employee security awareness training (for physical card handling)
2. Ensure strong physical security controls around payment devices
3. Review legacy environment for cardholder data storage and purge accordingly (or tokenize)
4. Document and monitor controls

### Recommended Comprehensive Solution

Element Payment Services has a comprehensive suite of PCI compliant solutions, referred to as a TransForm™ P2PE that addresses all of the Payment Solutions Selection Criteria, noted in this document, to ensure maximum merchant value and cardholder security.

**Hosted (SaaS) Solution: Express Processing Platform**

Express is Element’s secured, Software as a Service (hosted) payment processing platform that removes cardholder data from the merchant and ISVs network to the SAS 70 and PCI DSS validated host platform within Element. This hosted solution is a component of the product suite that forms the comprehensive point-to-point encryption solution. TDES Encryption is used to protect cardholder data while in transit from the entry point to the Express Processing Platform. Express integrates with ISVs’ business management software to accept cardholder data on behalf of the ISV and merchant. This platform is most often used with Ingenico devices and IDTech’s SecureKey enabled applications; however, Express is device agnostic and interoperable with nearly all PCI Compliant payment solutions.
**Tokenization: TransForm™ Tokenization Technology**

TransForm™ Tokenization is Element’s hosted and proprietary tokenization product which protects merchant’s need for transaction data. The solution works by moving the actual cardholder data offsite to Element’s PCI DSS compliant storage facility. Element’s servers create and then return a unique 36 character hexadecimal reference pointer (or token) to the merchant. Using the token (which contains no cardholder data); merchants can bill a card on file and schedule automatic payments. Element’s card tokenization solution is different from other implementations in that a token is produced per account rather than per transaction. Combining TransForm™ Tokenization with the Hosted Express Processing Platform creates a powerful cardholder data protection tool while enabling merchant’s ongoing ability to manage customer relations.

**ISV Business Management Software Integration**

Over 200 ISV software solutions are integrated with the Element Express Processing Platform. Express features TransForm™ P2PE and tokenization, making merchant payment acceptance and management simple and secure.

**Device Interoperability**

Element also provides a comprehensive line of encrypting, uni-directional, keyboard-emulated (driverless) point of entry solutions to ease implementation. ISVs incorporating TransForm™ devices into their fully integrated processing solution simply capture the XML message generated by the device (and defined by Element) which contains the non-sensitive and encrypted data needed to perform a payment transaction. The ISV’s application parses and transmits the data to the Element Express Processing Platform’s API for processing. Unlike other solutions where protocols vary between devices and require individual integration efforts, with TransForm™, integration is a one-time event. TransForm™, point of entry solutions utilize the same XML message format, allowing ISVs to offer the entire suite of devices after completing a single, simple integration. Merchant plug the device into a USB port on the point-of-sale system and begin processing encrypted, out-of-scope transactions without transmitting “readable” card data. This will eliminate the threat of malware attacks on the software application which attempt to steal credit and debit card information. Element’s hosted solution is device agnostic and interoperable with many encrypting payment devices.

The diagram on the right illustrates the significance of implementing Element's Hosted TransForm™ P2PE Suite (Hosted Express + PASS + Device/Application Agnostic) to reduce reliance on network segmentation and significantly limit PCI costs/scope along with the related liability.

Element’s hosted TransForm™ suite yields one of the most comprehensive P2PE solutions on the market today. Their solution suite ensures sensitive cardholder data is protected from the point of card swipe or entry, while in transit, all the way to the payment processor, and during storage. State of the art, point-of-entry devices encrypt both card present and card not present prior to performing a payment transaction. Even if the data were to be intercepted, it would be useless to cyber thieves as it is rendered “unreadable” and therefore has no value.

Source: ThoughtKey, Inc. proprietary analysis of payment solutions during 2008 to 2011.
A merchant selecting the comprehensive TransForm™ P2PE Suite offered by Element Payment Services gains quantifiable benefits that address continuous cyber threats while optimizing business operations and (protecting their brand).

- Element’s hosted TransForm™ P2PE solution suite is a forward-thinking solution that limits the scope of a merchant’s PCI audit (from over 220 to 6 PCI steps) and shifts responsibility and the related liability to Element as the hosted (SaaS) provider. These solutions represent an appealing combination to cost conscious merchants.

- The suite provides a proven effective encryption solution that allows merchants to reduce internal cardholder data storage and eliminate redundant PCI maintenance resources.

- This solution suite also enables ISVs to reduce their liability and costs by eliminating PCI DSS/PA-DSS validation requirements and card brand registration, by transferring the PCI burdens to Element as the hosted P2PE provider.

Element Payment Services’ TransForm™ P2PE Suite provides state of the art processing and protection. As data breaches continue to plague the payments industry and occupy headlines, our recommendation may become a mandate for merchants in the near future.

The payment industry is striving to reduce the quantity of cardholder data, or gold, available to thieves, along with the number of locations, or forts, where that gold is stored. Merchants themselves can win this battle by using Element’s TransForm™ P2PE Suite of solutions, which support a merchant’s operational needs and desire to preserve profit by eliminating unnecessary exposure to PCI costs and liability. The regulations and PCI standards support protection of the consumer.

Today, Element’s comprehensive solution is here to support merchant’s battle to preserve profit and protect their brand.

Susan Matt is CEO of ThoughtKey, a payment industry boutique consulting firm focused on PCI, regulatory compliance, risk management and expert testimony serving all parties of the payment industry value chain. www.thoughtkeyinc.com