First Data Market Insight

Reducing PCI DSS Scope with the First Data® TransArmor® Solution

Organizations who handle payment card data are obligated to comply with the Payment Card Industry Data Security Standard (PCI DSS.) The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.[1]

PCI DSS requirements apply to all system components that are included in or connected to the cardholder data environment (CDE). The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data, including terminals, network components, servers, and applications. Any device or application that process, transmits, or stores cardholder data and anything connected to those devices or applications is "in scope" for PCI DSS. This inclusive definition of what needs to be secured has made PCI DSS compliance a complex and costly endeavor for many merchants.

Scope reduction – the process of limiting or shrinking the CDE - is a way to reduce costs and effort associated with complying with PCI DSS. This whitepaper discusses how the TransArmor solution can enable scope reduction and ease the burden of PCI compliance.

[1] Definition from PCI Security Standards Council-
https: //www.pcisecuritystandards.org/security standards/pci dss.shtml

The First Data® TransArmor® solution delivers strong data security to merchants as a service as part of processing payment card transactions. The solution incorporates encryption and tokenization technologies to protect sensitive payment card data.

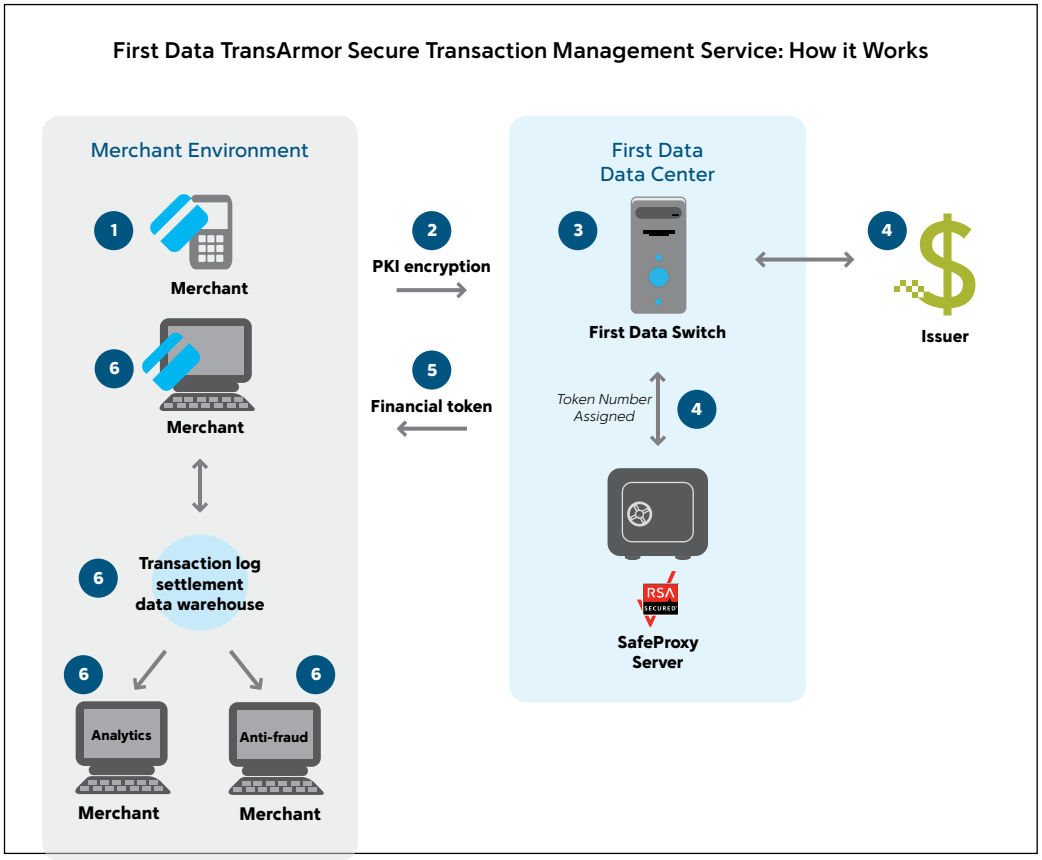
Following is an overview of how the TransArmor secure transaction management service works in a card-present environment:

1. When a purchase is made, the payment card number is captured and encrypted at the merchant's point of sale (POS) terminal. The TransArmor software on the merchant's POS terminal handles the encryption, which is asymmetric, meaning different keys are used for encryption than for decryption.

2. The encrypted card data is transmitted over secure networks to First Data.

3. First Data decrypts the Primary Account Number (PAN) using a secure private key.

4. First Data presents the merchant's transaction to the payment card brands (i.e., Visa, MasterCard, MAC, etc.) for authorization. Simultaneously, First Data checks the PAN against a table previously processed payment cards to see if a token number has already been assigned to the card number. If so, the existing token number assigned to that card is reused. If the payment



card hasn't been previously presented to First Data, then a new token number is randomly assigned to the PAN, and First Data logs which token corresponds to the new PAN for future transactions. First Data re-encrypts the PAN and stores it as ciphertext within a highly secure data vault.

5. First Data returns the payment authorization and the token number for the card to the merchant's POS, where the information is stored with related transaction and cardholder data (i.e., SKUs for items purchased, cardholder name).

6. The merchant uses the token number in other business processes, such as sales auditing, marketing analytics, loss prevention auditing and customer loyalty programs. Subsequent payment transactions, such as adjustments, refunds, "card not present" payments and delayed settlement, can also use the token in place of the card number.

Scope Reduction Drivers

On January 22, 2010, the PCI Security Standards Council (PCI SSC) provided guidance on the question "Is encrypted cardholder data considered cardholder data that must be protected in accordance with PCI DSS?" (Article #10359). The PCI SSC stated, "encrypted data may be deemed 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." Therefore, if a merchant encrypts cardholder data but does not possess the means to decrypt it, the cardholder data is not considered in scope once it has been encrypted.

Typically, merchants operating in-house encryption systems for payment card data don't benefit from reduced PCI scope, because the appiications and systems that use the card data must decrypt it to make it readable and usable. To take their encrypted card data environments outside the scope of PCI review, merchants must contract key management to an outside party, which, in turn, must prove it's able to protect cryptographic keys in accordance with industry best practices such as those specified by the NIST or in the PCI DSS.

The specific implementation of the TransArmor solution has several elements which enable users to remove card data from PCI scope. The use of public key encryption is one enabler. Track data is encrypted with the Public Encryption Key at the terminal and only the corresponding Private Encryption Key can be used to decrypt this data. Since the Merchant does not possess the Private Encryption Key, the Merchant "does not have the means to decrypt it." Per the PCI SSC guidance, this data, once encrypted, can be considered out of scope.

Tokenization of PAN data is the main enabler for scope reduction. The use of tokens for post-authorization operations (returns, chargebacks, recurring payments, sales reports, analytics or marketing programs) reduces the instances of storage of the PAN and takes applications and systems for these business processes which previously required PAN data out of scope as well.

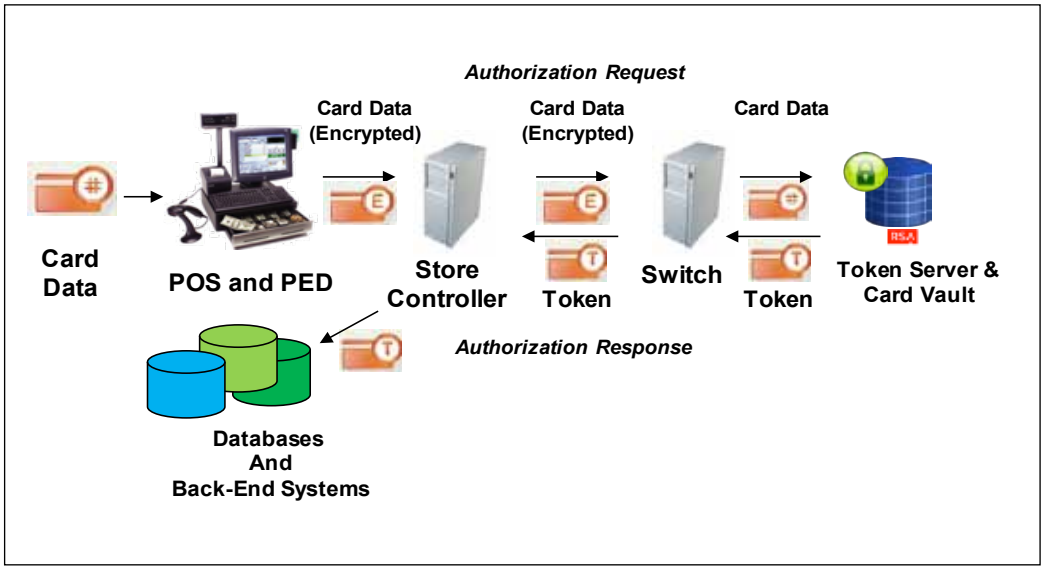
Another benefit of the TransArmor solution is that the payment processor is the only entity that the Merchant shares cardholder data with. The central database storing PANs and the systems with access to that database all reside outside the merchant's environment, meaning the service provider, not the merchant, bears the burden of proving adequate security for those systems. Since no cardholder data is being returned to the Merchant, any Service Providers that use the tokens for other business purposes or stores data for the Merchant would not be in scope.

With these concepts as a base, we will now look in detail at how use of the TransArmor solution may affect the completion of PCI DSS compliance questionnaires.

Affected PCI Requirements - SAQ-D

SAQ stands for "Self-Assessment Questionnaire"; SAQs must be completed by Merchants that are not required to undergo an on-site data security assessment and may be required by the merchant's acquirer or payment brand. Version D of the SAQ applies to Merchant who store cardholder data in electronic form. The SAQ-D contains the same requirements that the PCI DSS Audit Procedures contain, so this analysis also pertains to Merchants that are required to have an on-site PCI DSS assessment by a QSA.

The common layout of an SAQ-D Merchant performing card-present transactions, and the one that we'll focus on here, is a PED terminal that is physically connected to an Electronic Cash Register (POS) that is logically connected to a Controller somewhere in the store by switches, routers and/or firewalls. The credit card is swiped at the PED terminal, which then sends the transaction data to the ECR, which then sends the transaction data to the Controller, which then sends the transaction data to First Data. This is illustrated below.



Following is an examination of the PCI SAQ D questions that are affected by the adoption of the TransArmor solution:

1.3.7 Is the database placed in an internal network zone, segregated from the DMZ?

This requirement refers to a database that is being used to store the PAN. Since TransArmor returns a token in place of the PAN, the database would only be storing the token number. Due to this, this requirement would be considered not applicable to the Merchant.

3.1 (a) Is storage of cardholder data kept to a minimum, and is storage amount and retention time limited to that which is required for business, legal, and/or regulatory purposes?
(b) Is there a data-retention and disposal policy, and does it include limitations as stated in (a) above?

The TransArmor solution first encrypts the PAN with a Public Encryption Key, which renders the PAN out of scope outside of the PED terminal where the encryption is taking place, if for some reason it is being stored within the Merchant's network. Any storage of this encrypted PAN would thus be out of scope for these two requirements. Second, the TransArmor solution returns a token number in place of the PAN so any storage of the token would also be out of scope as the token is not considered to be cardholder data. Due to both of these TransArmor solution processes, these two requirements would be considered not applicable to the Merchant.

3.3 Is the PAN masked when displayed (the first six and last four digits are the maximum number of digits to be displayed)?

The TransArmor solution returns the token with only the last four digits of the PAN still intact. Therefore any displays (on the PED terminal, ECR, receipt, reports, etc.) will only be able to show the true last four digits of the PAN. This requirement would be considered in place (marked Yes) for the Merchant.

3.4 Is PAN, at a minimum, rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches?

- ♣ → **One-way hashes based on strong cryptography.**
- ♣ → **Truncation**
- ♣ → **Index tokens and pads (pads must be securely stored)**
- → **Strong cryptography with associate key management processes and procedures.**

The TransArmor solution returns a token number in place of the PAN. If the token were being stored, it would comply with this requirement according to the third bullet point. This requirement would therefore be considered in place (marked Yes) for this Merchant.

3.4.1 If disk encryption (rather than file- or column-level database encryption is used:
(a) Is logical access managed independently of native operating system access control mechanisms (for example, by not using local user account databases)?
(b) Are decryption keys independent of user accounts?

Since the TransArmor solution encrypts at the transaction stage and only the tokenized PAN is return, there would not be a need for disk encryption. Therefore these two requirements would be considered not applicable to the Merchant.

3.5 Are cryptographic keys used for encryption of cardholder data protected against both disclosure and misuse?

The TransArmor solution uses a Public Encryption Key to encrypt the cardholder data. Unlike symmetric encryption keys, Public Encryption Keys are made to be distributed widely and cannot be used to decrypt the data that it used to encrypt. For this reason, the Public Encryption Key does not need to be protected from disclosure or misuse as it is only half useful without the corresponding Private Encryption Key, which is housed at First Data and not at the Merchant. However, the Public Encryption Key is protected within the PED terminal. This requirement would be considered not applicable to the Merchant.

3.5.1 Is access to cryptographic keys restricted to the fewest number of custodians necessary?

As stated for requirement 3.5 above, the TransArmor solution uses a Public Encryption Key, which is made to be distributed widely and thus it does not need to be restricted to a few number of custodians. Further, each public key is signed with an X.509 certificate and terminals check the validity of the keys with a certificate authority in the First Data data center.

As for the Private Encryption Key, it is housed at First Data, it is owned by First Data and it is also protected and managed by First Data. Due to this, the Merchant is not responsible for the Private Encryption Key and cannot be assessed on it. This requirement would be considered not applicable to the Merchant.

3.5.2 Are cryptographic keys stored securely, and in the fewest possible locations and forms?

The Public Encryption Key that the TransArmor solution uses is injected into the Merchant's PED terminals and is stored securely within. It is only stored in one form and the number of locations depends on the number of PED terminals that the Merchant has. As described above, the keys are also signed and protected using X.509 certificates. This requirement would be considered in place (marked Yes) for the Merchant.

3.6 (a) Are all key-management processes and procedures for cryptographic keys used for encryption of cardholder data fully documented and implemented?
(b) Do they include the following?
3.6.1 Generation of strong cryptographic keys
3.6.2 Secure cryptographic key distribution
3.6.3 Secure cryptographic key storage
3.6.4 Periodic changing of cryptographic keys:
- → **As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically**
- → **At least annually**

3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys
3.6.6 Split knowledge and establishment of dual control of cryptographic keys
3.6.7 Prevention of unauthorized substitution of cryptographic keys
3.6.8 Requirement for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities.

The TransArmor Public and Private Encryption Keys are owned and managed by First Data, not the Merchant. Therefore the Merchant would not need to have procedures for the management of the encryption keys. These nine requirements would be considered not applicable to the Merchant.

4.1 Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?

Since the TransArmor solution encrypts the cardholder data at the PED terminal, it remains encrypted through transmission until it reaches First Data. Therefore, this requirement would be considered not applicable to the Merchant as the data is already encrypted prior to being transmitted over a public network. Alternative transport methods may be supported in the future, but they will all be standards such as SSL/TLS.

4.2 Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?

Since the TransArmor solution first encrypts at the PED terminal the PAN being sent to First Data and then only returns a tokenized PAN, unencrypted PAN would not be available outside of the PED terminal. In other words, there wouldn't be any unencrypted PAN available for employees to send via end-user messaging technologies. This requirement would be considered not applicable to the Merchant.

8.6.16 Is all access to any database containing cardholder data authenticated? (This includes access by applications, administrators, and all other users.)

As with requirement 1.3.7 above, this requirement refers to a database that is being used to store the PAN. Since the TransArmor solution returns a token number in place of the PAN, the database would only be storing the token. This requirement would be considered not applicable to the Merchant.

9.1.1 (a) Do video cameras or other access-control mechanisms monitor individual physical access to sensitive areas?
(b) Is data collected from video cameras reviewed and correlated with other entries?
(c) Is data from video cameras stored for at least three months, unless otherwise restricted by law?

Sensitive areas refer to "any data center, server room, or any area that houses systems that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in retail stores." Since the TransArmor solution returns a token number in place of the PAN, there would be no storage of cardholder data thus no data centers, server rooms or any other area would house systems that store cardholder data. These three requirements would be considered not applicable to the Merchant.

9.3 Are all visitors handled as follows:
9.3.1 Authorized before entering areas where cardholder data is processed or maintained?
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employees?
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration?
9.4 (a) Is a visitor log in use to maintain a physical audit trail of visitor activity?
(b) Are the visitor's name, the firm represented, and the employee authorizing physical access documented on the log?
(c) Is visitor log retained for a minimum of three months, unless otherwise restricted by law?

With the TransArmor solution, the cardholder data is processed only at the PED terminal that is located in the cashier area. Visitors there would consist of customers whom are always authorized to shop. Customers would not be required to have a physical access token and would not be required to sign a visitor log. These six requirements would be considered not applicable to the Merchant. However, a best practice is to educate employees to not let anyone take or administrate a PED terminal or Electronic Cash Register without proper authorization.

9.5 (a) Are media back-ups stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility?
(b) Is this location's security reviewed at least annually?

9.6 Are all paper and electronic media that contain cardholder data physically secure?
9.7 (a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?
(d) Do controls include the following:
9.7.1 Is the media classified so it can be identified as confidential?
9.7.2 Is the media sent by secured courier or other delivery method that can be accurately tracked?
9.8 Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)?
9.9 Is strict control maintained over the storage and accessibility of media that contains cardholder data?
9.9.1 (a) Are inventory logs of all media properly maintained?
(b) Are media inventories conducted at least annually?
9.10 Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons?
9.10.1 Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?
9.10.2 Is electronic media with cardholder data rendered unrecoverable so that cardholder data cannot be reconstructed?

With the TransArmor solution, no paper or electronic media would contain cardholder data, as only the token number, which is not considered cardholder data, would be stored on electronic media or printed on paper receipts, or reports. Therefore, these thirteen requirements would be considered not applicable to the Merchant.

10.2 Are automated audit trails implemented for all system components to reconstruct the following events:
10.2.1 All individual user accesses to cardholder data?

Since with the TransArmor solution only the token number is store, no user would have access to cardholder data. Audit trails would not need to be enabled in order to record this non-event. This requirement would be considered not applicable to the Merchant.

12.3.10 When accessing cardholder data via remote-access technologies, does the policy specify the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media?

The TransArmor solution returns a token in place of the PAN. The token is not considered to be cardholder data therefore employees would not have any cardholder data to access via remote-access technologies. This requirement would be considered not applicable to the Merchant.

It is important to note that the above analysis assumes that all existing storage of PAN data in the merchant environment has been eliminated or converted to token numbers.

Summary of Affected Items for SAQ-D:

PCI Requirement	Impact
1.3.7	Not Applicable
3.1 (a)	Not Applicable
3.1 (b)	Not Applicable
3.5	Not Applicable
3.5.1	Not Applicable
3.5.2	Yes / In Place
3.6	Not Applicable
3.6.1	Not Applicable
3.6.2	Not Applicable
3.6.3	Not Applicable
3.6.4	Not Applicable
3.6.5	Not Applicable
3.6.6	Not Applicable
3.6.7	Not Applicable
3.6.8	Not Applicable
4.1	Not Applicable
4.2	Not Applicable
8.5.16	Not Applicable
9.1.1 (a)	Not Applicable
9.1.1 (b)	Not Applicable
9.1.1 (c)	Not Applicable
9.3.1	Not Applicable
9.3.2	Not Applicable
9.3.3	Not Applicable
9.4 (a)	Not Applicable
9.4 (b)	Not Applicable
9.4 (c)	Not Applicable
9.5 (a)	Not Applicable
9.5 (b)	Not Applicable
9.6	Not Applicable
9.7 (a)	Not Applicable
9.7.1	Not Applicable
9.7.2	Not Applicable
9.8	Not Applicable
9.9	Not Applicable
9.9.1 (a)	Not Applicable
9.9.1 (b)	Not Applicable
9.10	Not Applicable
9.10.1	Not Applicable
9.10.2	Not Applicable
10.2.1	Not Applicable
12.3.10	Not Applicable

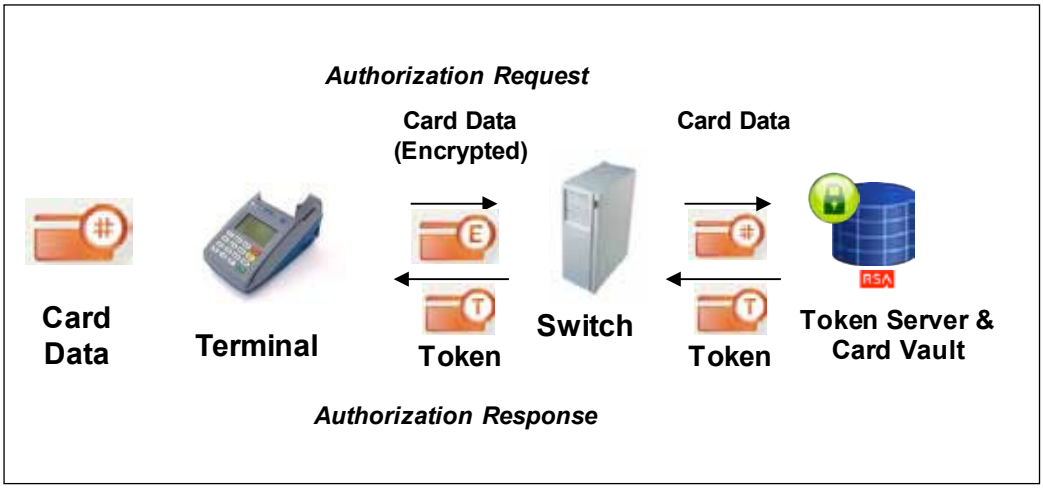
Affected PCI Requirements - SAQ- C

The Self-Assessment Questionnaire version C must be completed by Merchants that are not required to undergo an on-site data security assessment and that meet all five of the following criteria:

- → Merchant has a payment application system and an Internet or public network connection on the same device;
- → The payment application system/Internet device is not connected to any other system within the Merchant environment;
- → Merchant does not store cardholder data in electronic format;
- → If Merchant does store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; and
- → Merchant's payment application software vendor uses secure techniques to provide remote support to Merchant's payment application system.

It may be also be required by the merchant's acquirer or payment brand.

A common configuration of a SAQ-C Merchant performing card-present transactions is a standalone (a.k.a., countertop) PED terminal that is logically connected to First Data by DSL, cable modem or firewall. The credit card is swiped at the PED terminal, which then sends the transaction data directly to First Data. This is illustrated below.



Following is an examination of the PCI SAQ C questions that are affected by the adoption of the TransArmor solution:

3.2 Do all systems adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted)?

3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.

3.2.2 Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.

3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.

The PED terminal, where the credit card is swiped, stores the sensitive transaction data, which includes the track data, card-validation code and encrypted PIN block, in RAM (temporary memory) until the authorization is received. Afterwards, the PED terminal purges the sensitive transaction data. Since the PED terminal is not connected to any systems within the Merchant's network that have the possibility of storing the encrypted sensitive transaction data, these four requirements would be considered in place (marked Yes) for the Merchant.

3.3 Is the PAN masked when displayed (the first six and last four digits are the maximum number of digitsto be displayed)?

The TransArmor solution returns the token with only the last four digits of the PAN still intact. Therefore any displays (on the PED terminal, receipt, reports, etc.) will only be able to show the true last four digits of the PAN. This requirement would be considered in place (marked Yes) for the Merchant.

4.1 Are strong cryptography and security protocols, such as SSL/TLS or IPSEC, used to safeguard sensitive cardholder data during transmission over open, public networks?

Since the TransArmor solution encrypts the cardholder data at the PED terminal, it remains encrypted through transmission until it reaches First Data. Therefore, this requirement would be considered not applicable to the Merchant as the data is already encrypted prior to being transmitted over a public network.

4.2 Are policies, procedures, and practices in place to preclude the sending of unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat)?

Since the TransArmor solution first encrypts at the PED terminal the PAN being sent to First Data and then only returns a tokenized PAN, unencrypted PAN would not be available outside of the PED terminal. In other words, there wouldn't be any unencrypted PAN available for employees to send via end-user messaging technologies. This requirement would be considered not applicable to the Merchant.

5.1 Is anti-virus software deployed on all systems, particularly personal computers and servers, commonly affected by malicious software?

5.1.1 Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?

5.2 Are all anti-virus mechanisms current, actively running, and capable of generating audit logs?

The TransArmor solution is installed on the PED terminal, which is not a system that is commonly affected by malicious software. Since in order to be eligible to complete an SAQ-C the PED terminal cannot be connected to an Electronic Cash Register or a server, and is connected to First Data only through DSL, cable modem or a network device, these three requirements would be considered not applicable to the Merchant.

9.6 Are all paper and electronic media that contain cardholder data physically secure?

9.7 (a) Is strict control maintained over the internal or external distribution of any kind of media that contains cardholder data?

(d) **Do controls include the following:**

9.7.1 Is the media classified so it can be identified as confidential?

9.7.2 Is the media sent by secured courier or other delivery method that can be accurately tracked?

9.8 Are processes and procedures in place to ensure management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals)?

9.9 Is strict control maintained over the storage and accessibility of media that contains cardholder data?

9.10 Is media containing cardholder data destroyed when it is no longer needed for business or legal reasons?

9.10.1 Are hardcopy materials shredded, incinerated, or pulped so that cardholder data cannot be reconstructed?

With the TransArmor solution, no paper or electronic media would contain cardholder data, as only the token, which is not considered cardholder data, would be stored on electronic media or printed on paper receipts, or reports. Therefore, these eight requirements would be considered not applicable to the Merchant.

Summary of Affected Items for SAQ-C:

PCI Requirement	Impact
3.2	Yes / In Place
3.2.1	Yes / In Place
3.2.2	Yes / In Place
3.2.3	Yes / In Place
3.3	Yes / In Place
4.1	Not Applicable
4.2	Not Applicable
5.1	Not Applicable
5.1.1	Not Applicable
5.2	Not Applicable
9.6	Not Applicable
9.7 (a)	Not Applicable
9.7.1	Not Applicable
9.7.2	Not Applicable
9.8	Not Applicable
9.9	Not Applicable
9.10	Not Applicable
9.10.1	Not Applicable

Conclusion

Implemented properly, the TransArmor solution will enable users to remove selected card data and systems from PCI scope. The drivers for scope reduction are the solution's specific implementations of public key encryption and data tokenization. The resulting impact on PCI assessments can be significant, and merchants should engage with their QSA or other PCI experts to determine the impacts on their specific environments.

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.