Is TransArmor a listed Point to Point Encryption (P2PE) solution?  
No. TransArmor Data Protection (TADP) is not a listed P2PE solution, but it is still used for PCI DSS scope reduction as it effectively takes all elements with the exception of the terminal (or point of capture) out of scope for PCI DSS. TADP represents a superior solution to P2PE because it is an End to End Encryption (E2EE) solution – meaning there are no parties between the terminal and First Data that have access to the unencrypted PAN.

Which SAQ should I fill out if I am running TADP?  
That depends, however, First Data will accept SAQ B-IP for Levels 2 & 4 merchants as long as there are no other acceptance channels (such as paper, MOTO or eCommerce), and payment card numbers are not present in any other part of their environment. Proper handling of payment card data is the Merchant's responsibility. Submitting a compliant SAQ outside of these constraints will place the responsibility of a breach on the Merchant.

Why is TransArmor Data Protection’s E2EE superior to P2PE?  
With TADP’s E2EE, there are no parties in between the point of capture and First Data that can access the unencrypted payment card data. With P2PE, at least the P2PE gateway (and possibly others) have access to the raw transactional data, which increases the attack surface. In many cases, the P2PE gateway will forward the information to a processor like First Data in the clear, further exposing the data to disclosure.

If a breach were to occur at a P2PE gateway provider, the responsibility for the breach will fall to the merchant, as the acquirer has not taken possession of the data yet.

With TADP, because the transaction is decrypted by First Data, the transaction has added protection and is safer to process which benefits all parties.

Does a P2PE Solution need tokenization to be listed?  
No. Tokenization is not a requirement of a listed P2PE solution. TADP provides this important functionality by default to ensure that payment card data is never re-introduced into the merchant’s environment.

As a QSA, how should I validate the merchant-defined scope per PCI DSS if that merchant is using TADP?  
For merchants that use TADP, the scope should be defined as the terminals, and any other acceptance channel (such as eCommerce) that is part of the payment processing system and is outside of a terminal using TADP. In some cases, merchants may have non-TADP terminals for certain locations (such as, franchise) or they may use an eCommerce gateway that accepts and forwards transactions for that channel. Those would expand the scope. Merchants with manual entry processes (such as entry via a call center or other MOTO processes) should have those processes reviewed as well.
What types of encryption does TADP use?
TADP can be deployed to use one of three different kinds of encryption technologies: Verifone TAVE Encryption, RSA PKI, and 3DES-DUKPT. In every case, the technology is known to be a secure way to protect information, and TADP as well as other P2PE solutions use similar methods.

How does TADP manage tokens?
Tokens are managed at First Data using a token vault. Depending on the kind of token deployed, merchants will receive a random number back that will preserve certain elements of the original PAN (such as, the last four digits for receipt printing). This number has no mathematical relationship to the original PAN, so there is no way to decrypt the token. The token is then used to perform all future actions with the payment, including the option to initiate new payments (like a subscription) using the token after an initial authorization.

First Data maintains a 1:1 relationship between token and PAN, so the merchant will always get the same token back for any given PAN.

How are encryption keys managed?
Encryption keys for TADP are managed through Hardware Security Modules connected directly to the mainframes. For keys in the field, TADP uses RSA or PKI public keys, or each terminal will have keys specifically injected into them for processing.

Where is the data encrypted (SRED or Terminal App)?
Payment card data can be encrypted either inside the SRED reader or via an application embedded in the terminal that will capture it before processing. Once captured for encryption, the card will be protected during transmission to First Data systems.

Is there an implementation guide for TADP?
Yes, it is provided to the merchant.

What about Clover Gateway/Payeezy?
eCommerce transactions, when configured properly, are automatically protected with TADP. Those merchants will only see tokens in the Payeezy portal and would not have access to mass amounts of original payment data.