Case Studies

Point-to-Point Encryption

Implementation and Compliance Impacts of P2PE for Outdoor Fuel Retail

November 1, 2021

Version 1.0

Document Summary

This document provides use cases currently available in the industry showing how point-to-point encryption

Contributors

Alan Thiemann, Conexxus

Bruce Welch, Gilbarco

Brian Russell, Verifone

Christopher Mosser, Bennett Pump

Chuck Young, Impact 21

Dan Coates, ACI Worldwide

Dan Harrell, Invenco

Dennis Odiwo, ACI Worldwide

Jack Dickinson, Dover Fueling Solutions

Kevin Eckelkamp, Comdata

Kim Seufer, Conexxus

Mark Farver, Bennett Pump

Paul Kern, NCR

Sam Pfanstiel, Viking Cloud

Sean Gately, Bluefin

Sharon Scace, WEX

Simon Siew, Dover Fueling Solutions

Revision History

Revision Date	Revision Number	Revision Editor(s)	Revision Changes
November 1, 2021	1.0	Kim Seufer, Conexxus	Release Version
October 19, 2021	1.20	Kim Seufer, Conexxus	Updated Comdata diagram following TAC/SQA comments
October 4, 2021	1.19	Alan Thiemann, Conexxus Kim Seufer, Conexxus	Legal Review and reconcile comments from legal review
September 27, 2021	1.18	Kim Seufer, Conexxus	Updated based on comments from Comdata
August 3, 2021	1.17	Kim Seufer, Conexxus	Updated based on comments from Bluefin
June 15, 2021	1.16	Kim Seufer, Conexxus	Clean up comments
May 18, 2021	1.15	Sam Pfanstiel, Viking Cloud	Finalized case studies with case

			study participants
April 20, 2021	1.14	Kim Seufer, Conexxus	Updated formatting and accepted track changes
April 13, 2021	1.13	Brian Russell, Verifone Sam Pfanstiel, Viking Cloud Dennis Odiwo, ACI Worldwide	Added Verifone case study, updated ACI case study
March 7, 2021	1.12	Dan Coates, ACI Worldwide Sam Pfanstiel, Viking Cloud	Added ACI case study
June 22, 2020	1.11	Sam Pfanstiel, ControlScan	Merge 1.09.1, 1.10, and 1.10.1, added Invenco swimlane diagram
June 22, 2020	1.10.1	Simon Siew, Dover Fueling Solutions	Edits made to 1.10
June 19, 2020	1.09.1	Jack Dickinson, Dover Fueling Solutions	Edits made to 1.09
June 16, 2020	1.10	P2PE Working Group	Group revisions
June 16, 2020	1.09	Dan Harrell, Invenco Bruce Welch, Gilbarco Sam Pfanstiel, ControlScan	Added Invenco and Gilbarco case studies
May 26, 2020	1.08	Sam Pfanstiel, ControlScan	Finalized Bennett case study, submitted for working group review
May 18, 2020	1.07	Sam Pfanstiel, ControlScan	Added NCR case study, aligned content
April 23, 2020	1.06	Sam Pfanstiel, ControlScan	Added Bennett case study, finalized remaining content
October 20, 2019	1.05	Sam Pfanstiel, ControlScan	Incorporate case studies
August 19, 2019	1.04	Sam Pfanstiel, ControlScan	Edits
June 25, 2019	1.03	Sam Pfanstiel, ControlScan	Edits
May 14, 2019	1.02	Sam Pfanstiel, ControlScan Simon Siew, Dover Fueling Solutions	Dover case study
April 15, 2019	1.01	Sam Pfanstiel, ControlScan Kevin Eckelkamp, Comdata	COMDATA case study
February 21, 2019	1.00	Sam Pfanstiel, ControlScan Sharon Scace, WEX Chuck Young, Impact 21	Initial framework for case studies

Copyright Statement

This document contains copyrighted materials provided to Conexxus by the vendors whose use cases are found herein. Conexxus does not own the intellectual property (including rights) IPR in any of the data flows or diagrams or other works of authorship, or underlying technologies or solutions, provided by the vendors and described within this document ("Materials"). Such rights are expressly retained by the individual vendor. Conexxus has obtained a limited permission from each vendor to publish the respective Materials data flows and related information in this document, including all information herein; however, none of Materials, including this information, may be used for any purpose other than to evaluate the document user's P2PE procedures. The Materials data flow diagrams and vendor-specific information contained within this document may not be used for any other purpose, nor may any derivative works be created, without the permission of the individual vendor.

This document in its current form may be furnished to others, subject to the limited permission described above. All other uses must be pre-approved in writing by Conexxus (and the applicable vendor(s)). Moreover, this document may not be modified in any way, including removal of the copyright notice or references to Conexxus. Translations of this document into languages other than English shall continue to reflect the Conexxus copyright notice and the information contained in the Notice.

The limited permissions granted above are perpetual and will not be revoked specifically by Conexxus, Inc. or its successors or assigns.

Disclaimers

Neither Conexxus (nor the applicable vendor(s)) makes any no warranty, express or implied, about, nor does it assume any legal liability or responsibility for, the accuracy, completeness, or usefulness of any Materials information, product, or process described in the Materials. Although Conexxus uses reasonable best efforts to ensure this work product is free of any encumbrances resulting from third party intellectual property rights in this case, whereas disclosed above, individual vendors own the intellectual property rights surrounding the Materials found in this document. Accordingly, each user is encouraged to carefully review its implementation of these use cases and obtain appropriate licenses or permissions where needed.

Table of Contents

Project

Point-to-Point Encryption

Subtitle

P2PE Case Studies: Implementation and Compliance Impacts of P2PE for Fuel Retail.

1 Introduction and Overview

This document contains eight case studies that describe existing implementations of P2PE available for use in the fuel retail industry, including multiple automatic fuel dispenser (AFD) and unattended outdoor payment terminal (OPT) implementations, as well as a description of impacts on implementation, PCI P2PE compliance, PCI DSS compliance, and notes on implementation and user experience.

The intent of this document is to communicate how fuel retail merchants can implement a P2PE solution that improve security and reduce PCI compliance requirements and to facilitate cooperation among industry technology providers to increase such offerings for improved industry security and consumer cardholder data protection.

Where certain features for each technology or solution are designed to be customized per customer business requirements, these are described as “solution-specific.” In these cases, as with all implementations of payment security technology, the security impact may greatly depend on the specific configuration and oversight of the solution.

The Working Group wishes to express its gratitude to the many technology vendors who have shared specifics of their current and future capabilities to help inform the industry of these practice implementations of point-to-point encryption (P2PE) for outdoor fuel retail. As set forth in the Copyright Statement, no vendor has submitted its IP to Conexxus for this paper, but has given permission to provide the materials so the industry may consider ways to implement P2PE.

Conexxus also is not asserting that the case studies presented within this white paper are comprehensive of all solutions that may exist in the field. If a vendor wishes to be included in future revisions of this white paper, please contact support@conexxus.org.

1.1 Implementation Notes

Each solution depends upon the devices, cryptographic algorithms, key strengths, and key management processes supported by the hardware, software, and host processing entities. Merchants should understand that each of the case studies discussed are representative of one implementation among all possible configurations and they should consult with all applicable vendors for details and impacts on compatibility, security, and compliance.

2 Case Study – ACI Worldwide

ACI Worldwide (ACI) provides a P2PE solution that integrates with and leverages the capabilities of several POI manufacturers in the convenience and retail fuel space. In every ACI P2PE deployment, cardholder data is encrypted in the TRSM in the POI prior to transmission, and the encrypted data is decrypted at ACI's payment platform (which can be hosted by ACI, by the merchant, or third party) based on shared keys and the corresponding encryption algorithm. ACI Worldwide is a PCI-validated P2PE Solution Provider. ACI's validated solution utilizes select POIs within the various schemes it supports, so merchants who require validated P2PE should first consult with ACI to confirm their selected configuration matches one of the PCI-validated configurations.

2.1 Devices, Systems, and Service Providers

IPT POIs Supported:

- Ingenico
  - **Models:** Telium 2 and Tetra-based devices
  - **P2PE Schemes:** OnGuard, ACI P2PE (Telium only)
- PAX
  - **Models:** PxRetailer Compliant Devices (including several within the A Series, D Series, Q Series, Aries 6, Aries 8)
  - **P2PE Scheme:** PAX P2PE
- Verifone
  - **Models:** Vx and Mx Series, Engage Series
  - **P2PE Schemes:** Verifone Total Protect (VTP) (Passthrough only), Account Data Encryption (ADE)

OPTs POIs Supported:

- Wayne
  - **Models:** iXPay, iXPay 2
  - **P2PE Schemes:** RSA, VTP (Passthrough only)
- Gilbarco
  - **Models:** FlexPay II, FlexPay IV
  - **P2PE Schemes:** ACI-P2PE (3DES variant) (FlexPay IV only), VTP (Passthrough only)
- Invenco
  - **POI:** Invenco G6-300, G7UPC, G7 – 100 UPC
  - **P2PE Scheme:** ACI-P2PE

POS/EPS: Solution-Specific
P2PE Solution Providers: ACI Worldwide
Key Injection Facility: Verifone, Ingenico, Pax
Encryption Management: ACI Worldwide as P2PE Solution Provider
Encryption Scheme: Solution-Specific – see schemes listed for each device above.
The following schemes are 3DES DUKPT based: ACI P2PE, PAX P2PE, ADE, OnGuard
Decryption Management: ACI Worldwide as P2PE Solution Provider.
Processor: Any Processor – All decryption occurs on an ACI platform prior to routing.

Note: ACI technology can support other configurations, including deploying decryption to merchant's premises or to a third-party decryption provider, although such configurations would not be PCI-validated under the ACI P2PE Solution initially.

2.2 Data Flow Diagrams

ACI Payments Platform – Focus on P2PE

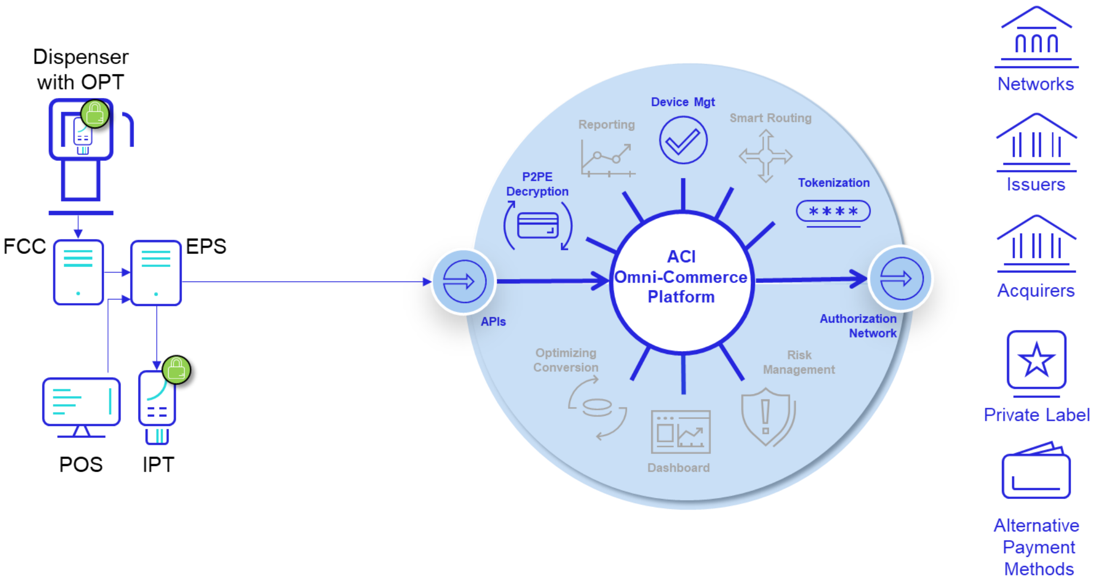


Figure 1A – ACI Worldwide-Supplied Architecture Diagram

In the above diagram, a typical C-Store configuration is shown. Note that in-store configuration is illustrative – actual configurations may vary. The key steps within the ACI P2PE solution are as follows:

1. The terminal driving system executes a standard checkout flow.
2. The POI encrypts the PCI-sensitive data within the SCD.
3. The data is carried via the site systems and transmitted to the ACI payments platform.

4. The platform decrypts the data before re-encrypting in a PCI DSS compliant manner routing it to the payment authorizing system.
5. In the response, ACI returns a token from its token vault, rather than the actual card data.

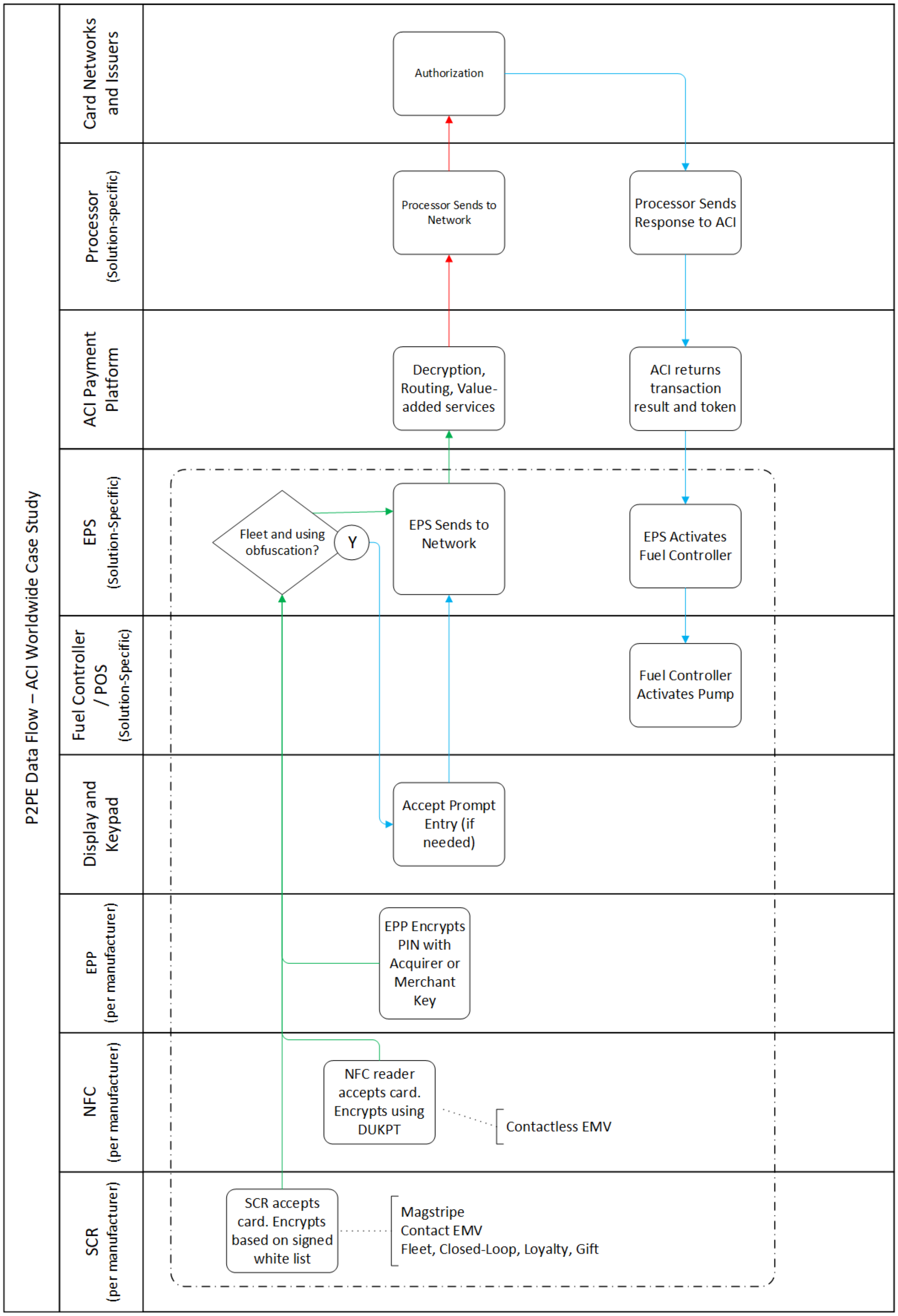

P2PE Data Flow – ACI Worldwide Case Study
Card Networks and Issuers
Processor (Solution-specific)
ACI Payment Platform
EPS (Solution-Specific)
Fuel Controller / POS (Solution-Specific)
Display and Keypad
EPP (per manufacturer)
NFC (per manufacturer)
SCR (per manufacturer)
Authorization
Processor Sends to Network
Processor Sends Response to ACI
Decryption, Routing, Value-added services
ACI returns transaction result and token
Fleet and using obfuscation?
Y
EPS Sends to Network
EPS Activates Fuel Controller
Fuel Controller Activates Pump
Accept Prompt Entry (if needed)
EPP Encrypts PIN with Acquirer or Merchant Key
NFC reader accepts card. Encrypts using DUKPT
Contactless EMV
SCR accepts card. Encrypts based on signed white list
Magstripe
Contact EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 1B – ACI Worldwide Data Flow for Use in P2PE Solutions

2.3 Impacts by Card Type

ACI’s P2PE solution manages each of the following card use cases as described below:

2.3.1 Consumer Branded

Consumer branded cards are always encrypted in the PED, unless the BIN of the card is included the BIN Whitelist file. Under the PCI-validated P2PE solution, ACI manages the BIN Whitelist to ensure PCI-branded cards are never left unencrypted. If a transaction is received at the ACI data center for processing with card data in the clear and that card is not represented in the BIN Whitelist file, the transaction will be declined at the ACI platform and terminal shall be marked as compromised.

2.3.2 Fleet

Fleet cards may be handled using one of the following four (4) options.

2.3.2.1 Whitelisting of Fleet Cards

The merchant may choose to whitelist all fleet cards for networks that do not align with the PCI Council. Track-based prompts may be processed by the site systems (EPS, FCC or other) and included in the transaction upstream to the payments platform.

2.3.2.2 Encrypt using P2PE, expose track-based prompt values

ACI’s P2PE standard utilizes a flexible whitelist mechanism whereby different card BINs may be masked using different obfuscation schemes. These various schemes enable fleet cards to be encrypted using P2PE yet expose critical business-needed values for fleet prompting. ACI’s P2PE standard supports the following schemes:

- Standard Obfuscation (masked PAN exposes first 6, last 4, expiry date, restriction code)
- No Obfuscation (i.e., whitelisted)
- Visa Fleet
- Mastercard Fleet
- FleetOne
- Voyager
- WEX

2.3.2.3 Encrypt using P2PE, payment platform returns prompts

With this option, all cards are encrypted using the device’s configured P2PE scheme. For cards that require prompting, the ACI payments platform identifies the prompt needed and returns a response to the upstream system indicating the prompt needed to proceed.

2.3.2.4 Host-based Prompting

Certain cards, especially those within the commercial fleet domain, are subject to host-based prompting. The prompts required are determined at the downstream host and returned to the upstream system. ACI supports this prompting mechanism.

2.4 Security and Compliance Impacts

2.4.1 Security Impact

Since card data is encrypted in the POI, ACI's P2PE solution ensures that merchants never have to deal with clear card data in their environments. This significantly reduces the threat of card data breach in the merchant's environment. In addition, ACI can provide a merchant- or card-specific format-preserving token that can be used for merchant related tasks, which require card numbers that have now been removed from the merchant's environment as a result of P2PE.

2.4.2 PCI P2PE Compliance Impacts

ACI's P2PE solution uses only PTS-approved devices, KIFs, encryption and decryption management, and schemes that have undergone validation as part of a PCI-validated P2PE solution. Merchants, distributors, or oil brands that wish to validate their own solution (including merchant-managed solutions) using ACI Worldwide services, may wish to contact ACI to determine suitability for undergoing a separate P2PE validation.

2.4.3 PCI DSS Compliance Impacts

Merchants that have deployed supported POIs and schemes that have been validated as part of the ACI P2PE solution and follow the provided P2PE Instruction Manual may enjoy the reduced PCI scope that is associated with deploying a validated solution, including eligibility to complete the SAQ P2PE.

3 Case Study – Bennett SSP5 – Automated Fuel Dispenser

The Bennett Pump Simply Secure Payment 5 (SSP5) system incorporates Magtek encrypting secure card reader (SCR), contactless (NFC), and encrypting pin pad (EPP), which are each injected with unique Magtek or acquirer keys. PIN data is encrypted by the EPP using acquirer keys and never unencrypted. Encrypted cardholder data are transmitted within the UPT enclosure to a central SCD that performs re-encryption to the acquirer's encryption specification. This configurable architecture is highly dependent upon the solution implementation to support various encryption standards and specifications.

3.1 Devices, Systems, and Service Providers

POI: Bennett SSP5 UPT (pending PTS validation):

- **SCR:** Magtek oDynamo – MSR, ICCR (Contact chip EMV) (SRED)
- **NFC:** Magtek Dynawave (non-SRED)
- **EPP:** Cryptera 1215

POS/EPS: Solution-Specific
P2PE Solution Provider: None at this time
Encryption Management: Solution-Specific
Encryption Scheme: Solution-Specific
Decryption Management: Solution-Specific
Processor: Solution-Specific

3.2 Data Flow Diagrams

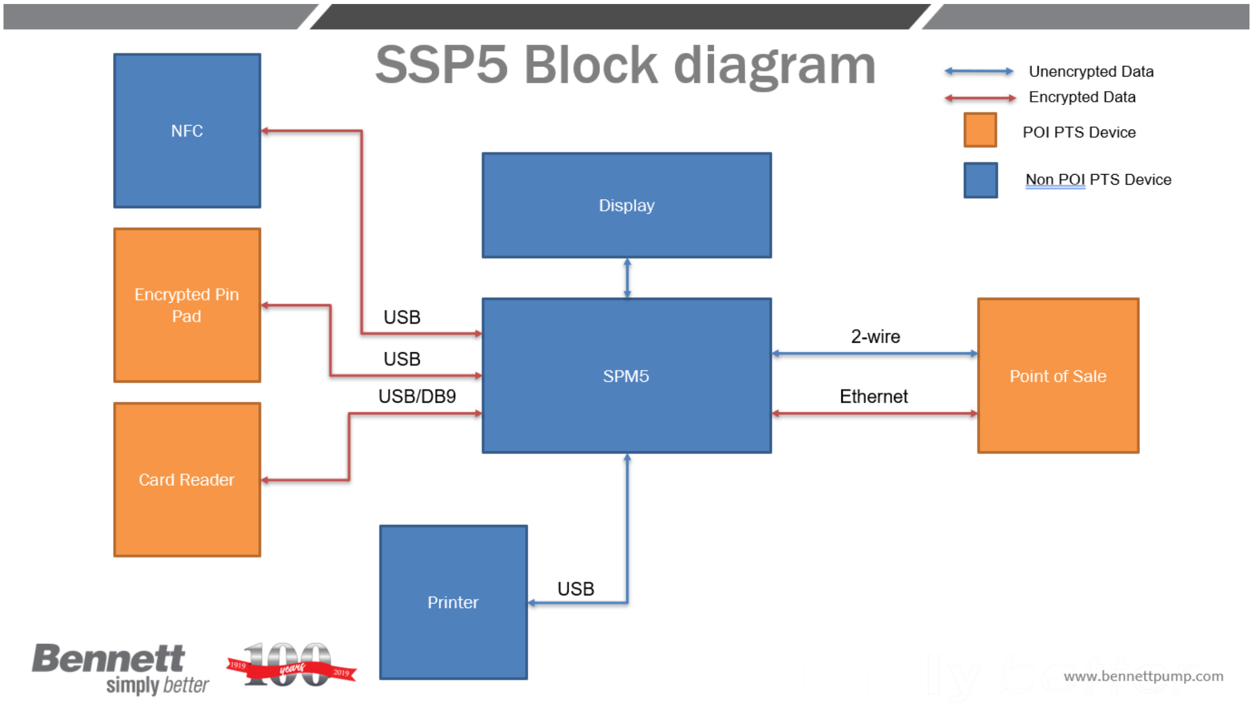


Figure 2A – Bennett Pump-Supplied Architecture Diagram

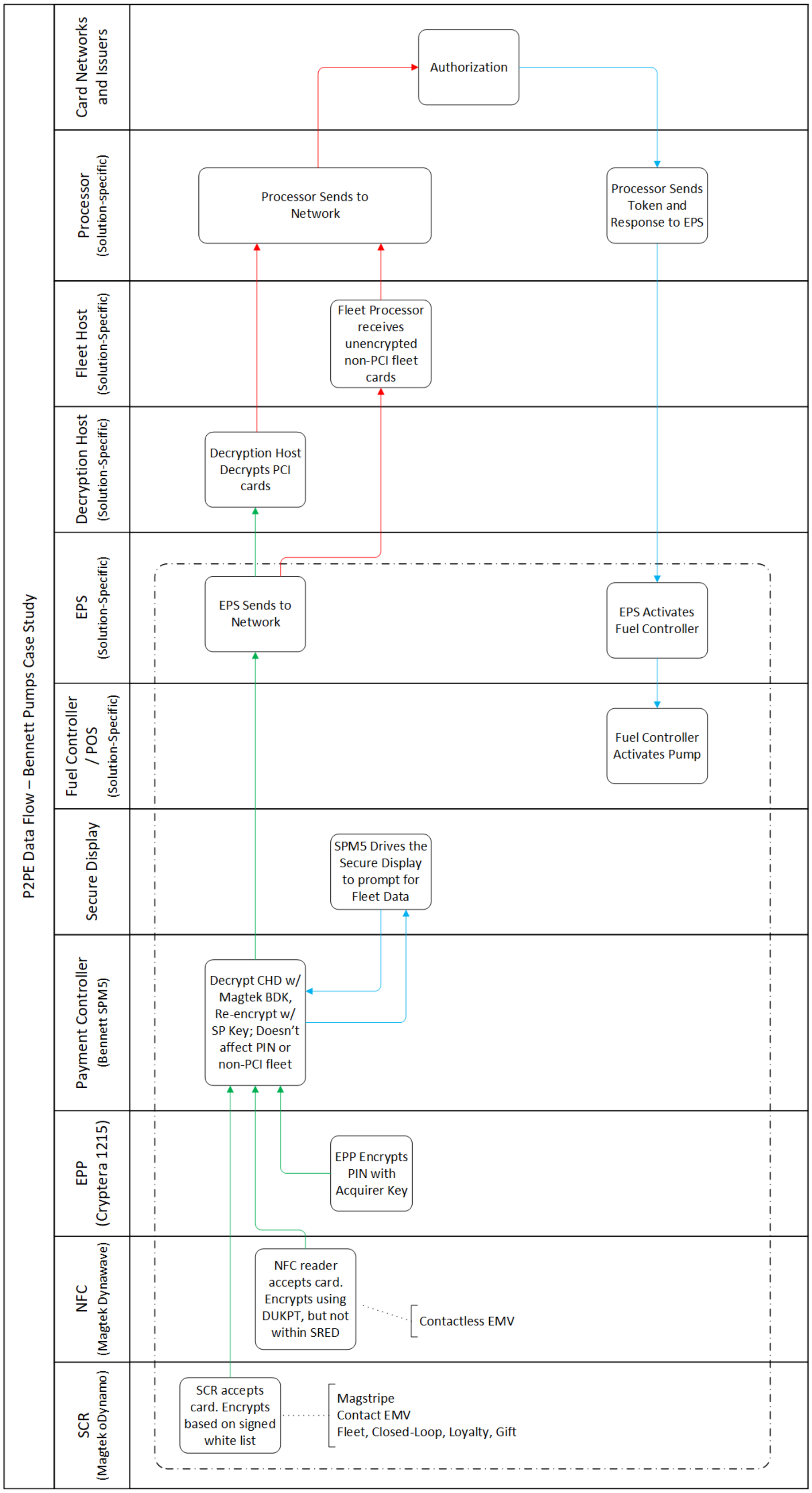

P2PE Data Flow – Bennett Pumps Case Study
Card Networks and Issuers
Processor (Solution-specific)
Fleet Host (Solution-Specific)
Decryption Host (Solution-Specific)
EPS (Solution-Specific)
Fuel Controller / POS (Solution-Specific)
Secure Display
Payment Controller (Bennett SPM5)
EPP (Cryptera 1215)
NFC (Magtek Dynawave)
SCR (Magtek oDynamo)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
Fleet Processor receives unencrypted non-PCI fleet cards
Decryption Host Decrypts PCI cards
EPS Sends to Network
EPS Activates Fuel Controller
Fuel Controller Activates Pump
SPM5 Drives the Secure Display to prompt for Fleet Data
Decrypt CHD w/ Magtek BDK, Re-encrypt w/ SP Key; Doesn't affect PIN or non-PCI fleet
EPP Encrypts PIN with Acquirer Key
NFC reader accepts card. Encrypts using DUKPT, but not within SRED
Contactless EMV
SCR accepts card. Encrypts based on signed white list
Magstripe
Contact EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 2B – Bennett Pump Data Flow for Use in P2PE Solutions

3.3 Impacts by card type

This solution manages each of the following card use cases as described below:

3.3.1 Consumer Branded

The Bennett architecture allows for flexible configuration, depending upon the merchant and solution implementation requirements. All card data is encrypted using Magtek keys by the SCR, NFC, and EPP prior to transmission to the SPM5 SCD. The SCR supports the use of a signed BIN whitelist.

The SPM5 SCD within the UPT enclosure supports the use of a signed BIN whitelist, which should be configured to ensure all PCI-branded consumer cards prior to transmission to the POS. POS support for encrypted account data is required for this implementation.

The signed BIN whitelist may be leveraged to leave non-PCI-branded consumer card unencrypted if required by the POS or processing host.

3.3.2 Fleet

The SSP5 supports fleet prompting using the secure display and may be configured based on the specific implementation requirements. Note that any PCI-branded fleet information that must be left unencrypted through the use of a BIN whitelist may expose the merchant to additional PCI DSS scope, as any such cards may be exposed within the merchant environment, and therefore vulnerable to interception.

3.4 Security and Compliance Impacts

The SSP5 supports multiple acquirer and solution implementations. The secure SSP5 enclosure and SPM5 SCD support multiple encryption approaches, and thus the ultimate security and compliance of any solution is highly dependent upon implementation:

3.4.1 Security Impact

All cardholder data and PIN encryption keys used within the SSP5 UPT are protected using 3DES DUKPT and/or AES128 and are securely loaded by the manufacturer within a secure key injection facility. The SSP5 secure perimeter provides a secure enclosure for all components and cryptographic operations and includes tamper-response mechanisms to protect keys and sensitive operations. Properly configured, the SSP5 ensures encryption of all cardholder data, reducing risk and improving security of these data in the fuel dispenser.

3.4.2 PCI P2PE Compliance Impacts

At the time of publication, the SSP5 is not yet a PTS-approved UPT device. However, upon approval, this device will support SCR-approved interfaces for card capture through the enclosed Magtek oDynamo, but not for NFC capture using the enclosed Magtek Dynawave. PCI-P2PE requires the use of SRED for all capture interfaces, so any solution provider that wishes to support the SSP5 in a validated solution must administratively disable the NFC interface such that the merchant cannot re-enable it.

In addition, the Magtek devices are injected with Magtek keys, and thus these keys and injection processes would also need to be reviewed for compliance to relevant PCI P2PE standard and testing requirements.

Finally, any such solution would require documentation on the internal use of Magtek and solution provider/acquirer keys to ensure all such operations are compliant with minimum cryptographic algorithm and key strength requirements.

3.4.3 PCI DSS Compliance Impacts

The SSP5 is not available within a PCI P2PE solution, and thus any implementation would require review by a knowledgeable QSA or QSA(P2PE) to confirm impact on the merchant's PCI DSS control and environmental scope. It is also recommended that merchants to consult with their acquirer to confirm approval for any scope determination that reduces the scope of PCI DSS through the use of encryption.

4 Case Study – COMDATA - Unattended Fuel Dispenser

The COMDATA SmartSite GX is a combined outdoor payment terminal (OPT) and site controller solution, providing an unattended POS platform for outdoor fueling. This solution utilizes a PCI Validated P2PE Solution Provider and components to handle all aspects of key injection and management, as well as encryption and decryption services in order to meet the requirements for PCI P2PE.

4.1 Devices, Systems, and Service Providers

This case study relates to the configuration consisting of the following technologies. Additional solution-specific technologies or vendors may also be present:

OPT POIs Supported:

- **SCR:** IDTech VP5300 – MSR, ICCR (Contact chip EMV)
- **NFC:** IDTech VP5300 antenna
- **EPP:** IDTech SmartPIN L100

Pumps Supported:

- **Gilbarco**: Various
- **Wayne**: Various

OPT: COMDATA SmartSite OPT (Outdoor Payment Terminal)

P2PE Solution Provider: Bluefin P2PE (PCI-Validated P2PE Solution)

Secure Payment Gateway Provider: PDI Security Solutions (Echosat)

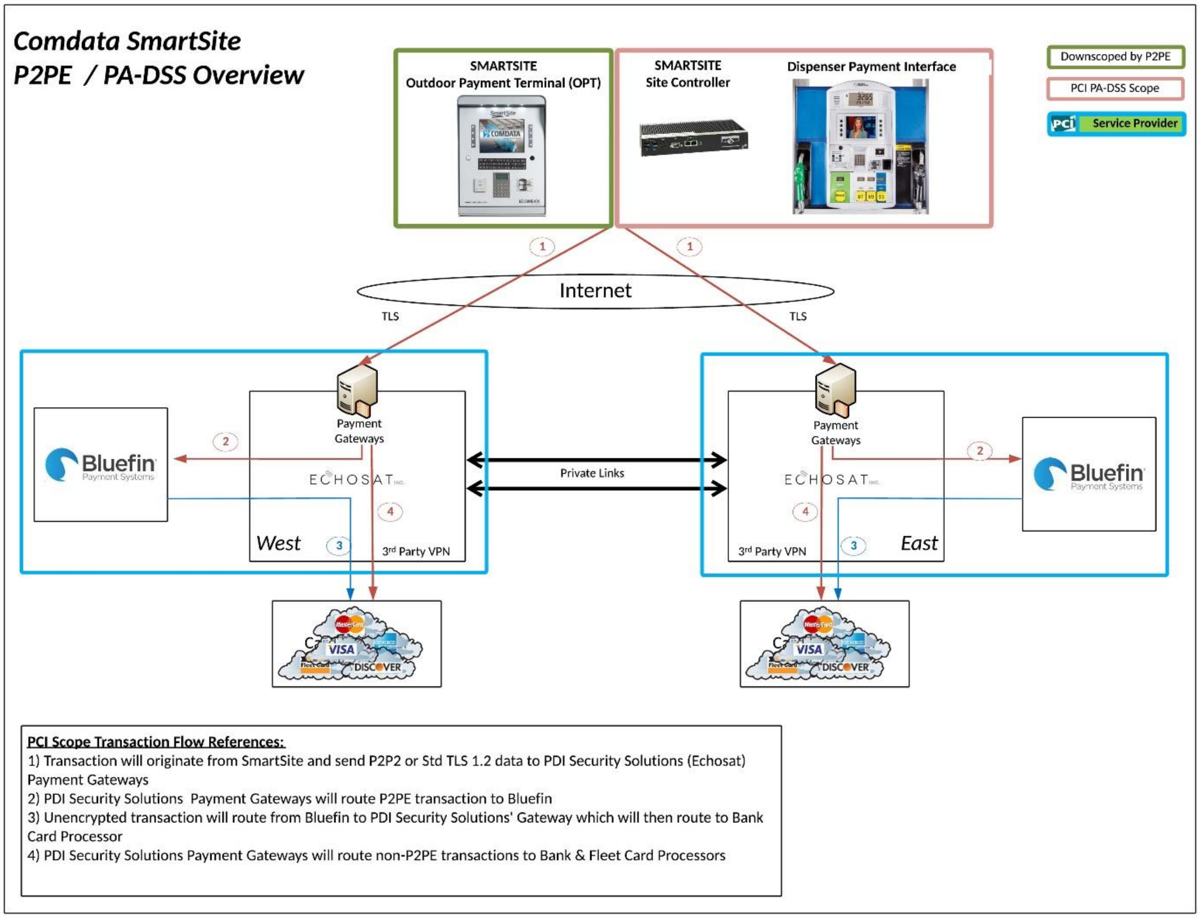
Encryption Management: Bluefin P2PE Manager (PCI-Validated P2PE Component)

Encryption Scheme: 3DES DUKPT

Network: PDI

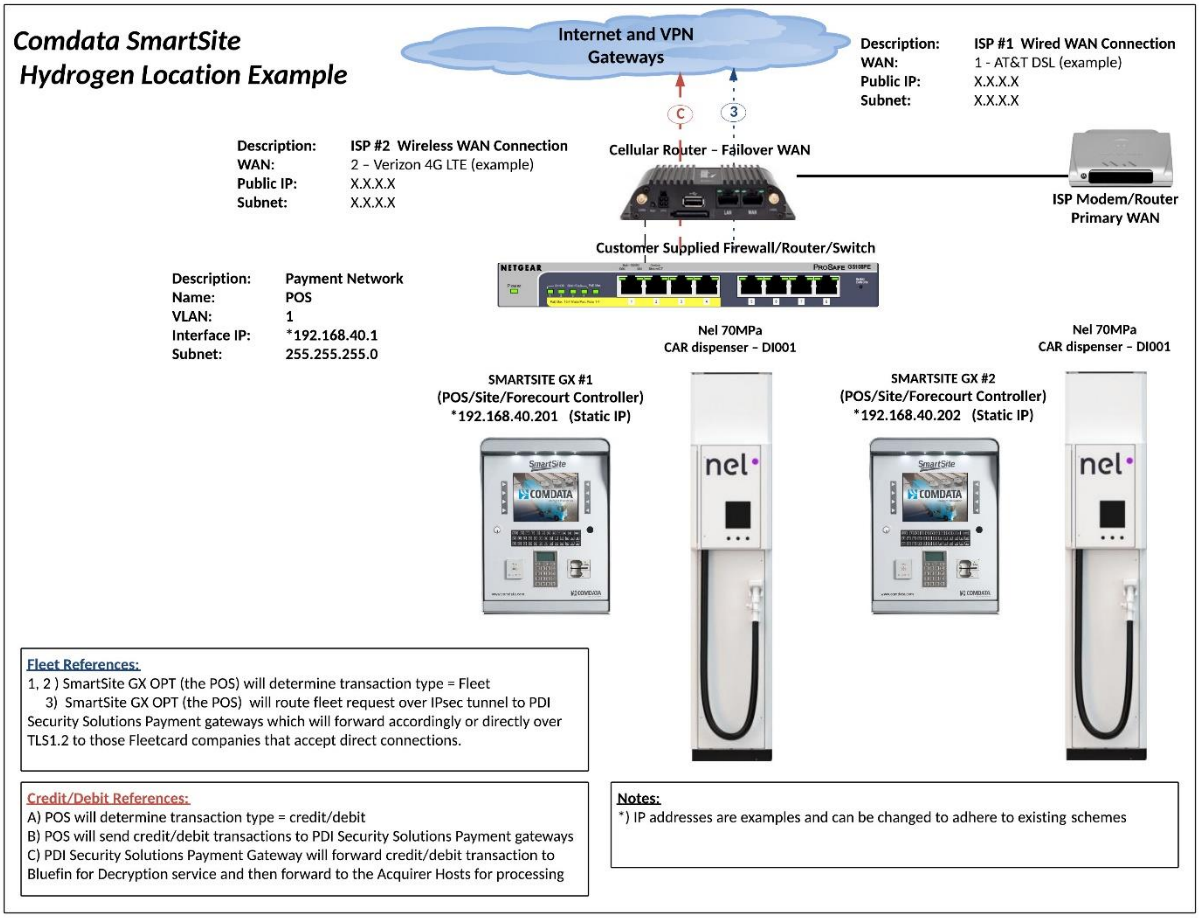
Decryption Management: Bluefin P2PE Cloud HSM (PCI-Validated P2PE component)

4.2 Data Flow Diagrams



PCI Scope Transaction Flow References:

1) Transaction will originate from SmartSite and send P2P2 or Std TLS 1.2 data to PDI Security Solutions (Echosat) Payment Gateways
2) PDI Security Solutions Payment Gateways will route P2PE transaction to Bluefin
3) Unencrypted transaction will route from Bluefin to PDI Security Solutions' Gateway which will then route to Bank Card Processor
4) PDI Security Solutions Payment Gateways will route non-P2PE transactions to Bank & Fleet Card Processors



Comdata SmartSite Hydrogen Location Example

Internet and VPN Gateways
C
3
Cellular Router – Failover WAN
ISP Modem/Router Primary WAN
Customer Supplied Firewall/Router/Switch
NETGEAR
ProSafe GS108PE
Nel 70MPa CAR dispenser – DI001
Nel 70MPa CAR dispenser – DI001
SMARTSITE GX #1 (POS/Site/Forecourt Controller) *192.168.40.201 (Static IP)
SMARTSITE GX #2 (POS/Site/Forecourt Controller) *192.168.40.202 (Static IP)
nel
SmartSite
COMDATA

Description:	**ISP #1 Wired WAN Connection**
WAN:	1 - AT&T DSL (example)
Public IP:	X.X.X.X
Subnet:	X.X.X.X

Description:	**ISP #2 Wireless WAN Connection**
WAN:	2 – Verizon 4G LTE (example)
Public IP:	X.X.X.X
Subnet:	X.X.X.X

Description:	**Payment Network**
Name:	**POS**
VLAN:	**1**
Interface IP:	***192.168.40.1**
Subnet:	**255.255.255.0**

Fleet References:

1, 2) SmartSite GX OPT (the POS) will determine transaction type = Fleet

3) SmartSite GX OPT (the POS) will route fleet request over IPsec tunnel to PDI Security Solutions Payment gateways which will forward accordingly or directly over TLS1.2 to those Fleetcard companies that accept direct connections.

Credit/Debit References:

A) POS will determine transaction type = credit/debit

B) POS will send credit/debit transactions to PDI Security Solutions Payment gateways

C) PDI Security Solutions Payment Gateway will forward credit/debit transaction to Bluefin for Decryption service and then forward to the Acquirer Hosts for processing

Notes:

*) IP addresses are examples and can be changed to adhere to existing schemes

Figure 3A – Comdata-Supplied Architecture Diagrams

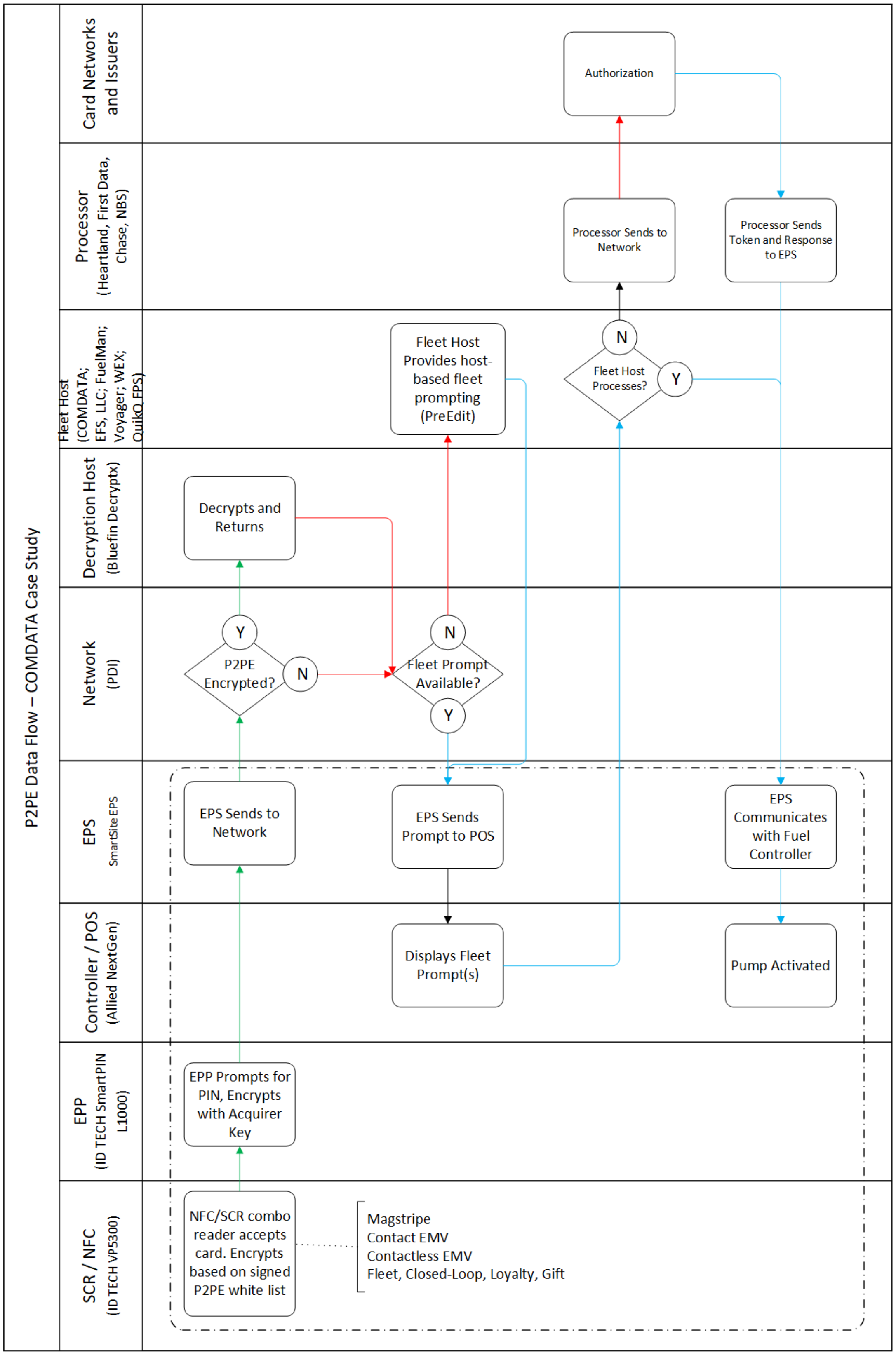

P2PE Data Flow – COMDATA Case Study
Card Networks and Issuers
Processor (Heartland, First Data, Chase, NBS)
Fleet Host (COMDATA; EFS, LLC; FuelMan; Voyager; WEX; QuikQ FPS)
Decryption Host (Bluefin Decryptx)
Network (PDI)
EPS SmartSite EPS
Controller / POS (Allied NextGen)
EPP (ID TECH SmartPIN L1000)
SCR / NFC (ID TECH VP5300)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
Fleet Host Provides host-based fleet prompting (PreEdit)
Fleet Host Processes?
N
Y
Decrypts and Returns
P2PE Encrypted?
Y
N
Fleet Prompt Available?
N
Y
EPS Sends to Network
EPS Sends Prompt to POS
EPS Communicates with Fuel Controller
Displays Fleet Prompt(s)
Pump Activated
EPP Prompts for PIN, Encrypts with Acquirer Key
NFC/SCR combo reader accepts card. Encrypts based on signed P2PE white list
Magstripe
Contact EMV
Contactless EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 3B – Comdata Data flow for use in P2PE solution

4.3 Impacts by Card Type

This solution manages each of the following card use cases as described below:

4.3.1 Consumer Cards

PCI-branded cards are encrypted within the IDTech VP5300 SCD/NFC antenna using SRED, prior to being passed to the network, decryption host, and processor. The VP5300 supports the use of a BIN whitelist, which is managed by Bluefin to ensure all PCI-branded cards are encrypted at the point of interaction.

Non-PCI-branded consumer cards will be encrypted unless they are contained in the BIN whitelist, which is maintained by Bluefin. Such allowances would be not be redirected to the Bluefin decryption system, and thus pass to the processing host as usual.

4.3.2 Fleet

Host-based fleet prompting for non-PCI-branded fleet cards is unaffected, as these “pre-edit” messages are passed directly to the fleet host with unencrypted cardholder data.

Host-based fleet prompting for PCI-branded fleet cards is supported, as these messages are first routed by the PDI network to the Bluefin decryption host, decrypted, returned to PDI, then passed to the fleet host with unencrypted cardholder data. The fleet host thus has access to all necessary account data and can return prompts using existing, standard methods. This method is called “P2PE decrypt/pre-edit”.

BIN-based fleet prompting is similarly unaffected, as the BIN is left unencrypted by the ID Tech POI. Any such changes to the BIN whitelist must be performed by Bluefin as the P2PE solution provider.

Fleet prompting for PCI-branded cards that rely upon discretionary data or track equivalent data (EMV) would leaving these data unencrypted would depend upon brand or issuer exception. Currently this exception may be available for Mastercard fleet cards, but not currently implemented.

All such implementations should be confirmed and tested with the appropriate fleet host and any BIN exclusions approved by the P2PE solution provider.

4.4 Security and Compliance Impacts

The COMDATA solution uses ID Tech PTS devices equipped with SRED encryption operations within the secure module of devices to protect account data immediately at card capture through the merchant environment, and only allows whitelisting for non-

PCI cards. This method of encryption ensures that the card is never decrypted within the merchant environment.

4.4.1 Security Impact

The use of 3DES DUKPT injection and encryption ensures a unique initial key per terminal, and unique encryption key for each transaction. As with any card-present solution, external skimmers may still be a threat which may access account data before it is encrypted by the POI.

4.4.2 PCI P2PE Compliance Impacts

All PCI-branded cards are encrypted by the SRED function within the secure module of the PTS POI, as tested within the PCI-validated P2PE solution. Encryption management is supported by the Bluefin Encryption Management component, including support for the Bluefin P2PE Manager. As such, these data are confirmed to be protected from eavesdropping once they pass into the device. The solution employs a routing mechanism provided by PDI, which detects encrypted account data, holds the transmission while it forwards the encrypted account data to the PCI-validated decryption management component provider, which securely returns decrypted account data to PDI for routing to payment processors. This substitution occurs by PCI-compliant third-party service providers downstream from the merchant, and therefore does not impact the exposure of cardholder data for the individual merchant location.

The COMDATA implementation uses PCI P2PE supported devices and PCI P2PE validated elements for key injection and management, as well as for encryption and decryption management. When implemented properly – including following the Bluefin PIM and using only approved devices and component providers – this channel may be considered a compliant implementation of a PCI P2PE solution as described below:

Solution Provider: Bluefin Payment Systems
Solution Name: Bluefin P2PE
Reference #: 202019-00897.0174

4.4.3 PCI DSS Compliance Impacts

All major card brands provide PCI DSS scope reduction for merchants that use PCI-listed P2PE solutions. However, the eligibility for this scope reduction is dependent upon the implementation of the P2PE solution according to the P2PE Instruction Manual provided by the P2PE Solution Provider, Bluefin Payment Systems. Small merchants who meet the eligible criteria may qualify to submit the SAQ P2PE, which comprises 33 total questions. Level 1 merchants would also qualify for equivalent scope reduction within their annual Report on Compliance (ROC).

5 Case Study – Dover Wayne iX Pay – Automatic Fuel Dispenser

The use of the PTS-approved iX Pay line of unattended payment terminal (UPT) PIN Transaction Security (PTS) devices provides account data encryption within an enclosed housing at each automated fuel dispenser (AFD). The second version in this series, iX Pay 2, can support a PCI-validated P2PE solution due to the use of unique encryption keys per terminal.

5.1 Devices, Systems, and Service Providers

This case study relates to the configuration consisting of the following technologies. Additional solution-specific technologies or vendors may also be present:

OPT POIs Supported:

- **UPT:** Dover Wayne iX Pay UPT
- **UPT:** Dover Wayne iX Pay 2 UPT

Pumps Supported:

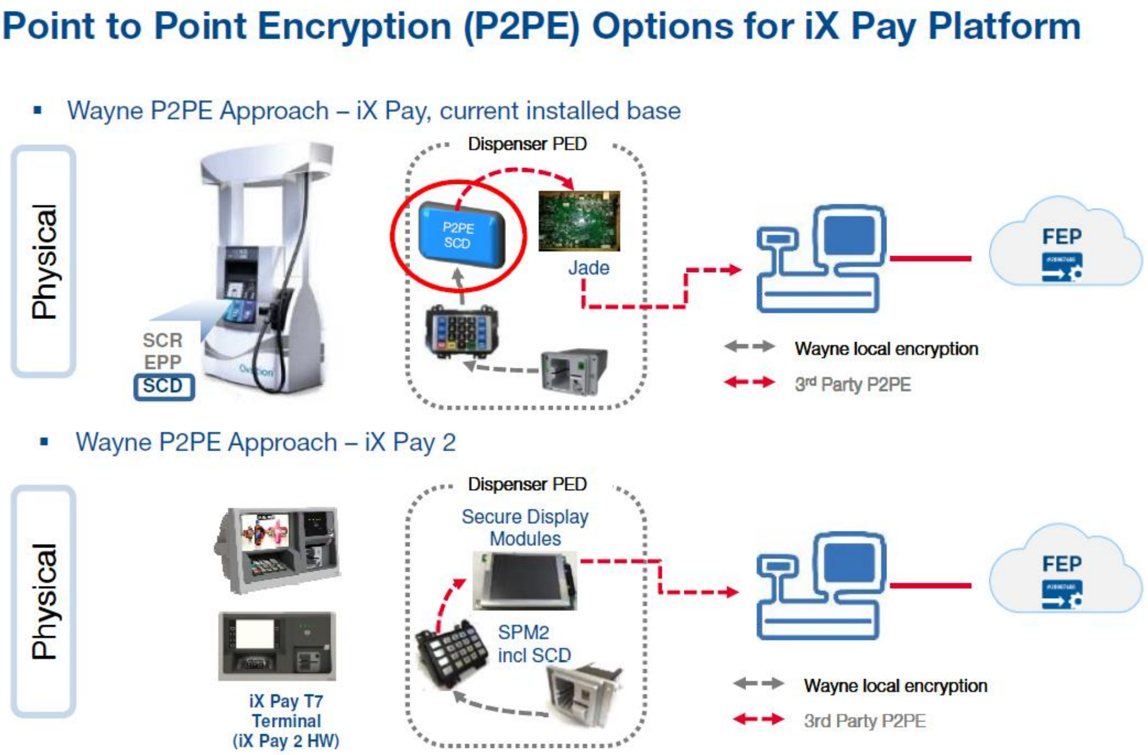
Gilbarco: Advantage, Encore 300/500, Encore 500S/700S
Wayne: Vista 1/2/3/4, Ovation 1 & 2, Helix, Anthem

Encryption Schemes: TransArmor VeriShield, RSA, DUKPT

Decryption Management: First Data TransArmor, OSAE

Processor: First Data, Solution-specific

5.2 Data Flow Diagrams



Point to Point Encryption (P2PE) Options for iX Pay Platform

- Wayne P2PE Approach – iX Pay, current installed base

- Wayne P2PE Approach – iX Pay 2

Figure 4A – Dover Fueling Solutions-Supplied Architecture Diagram

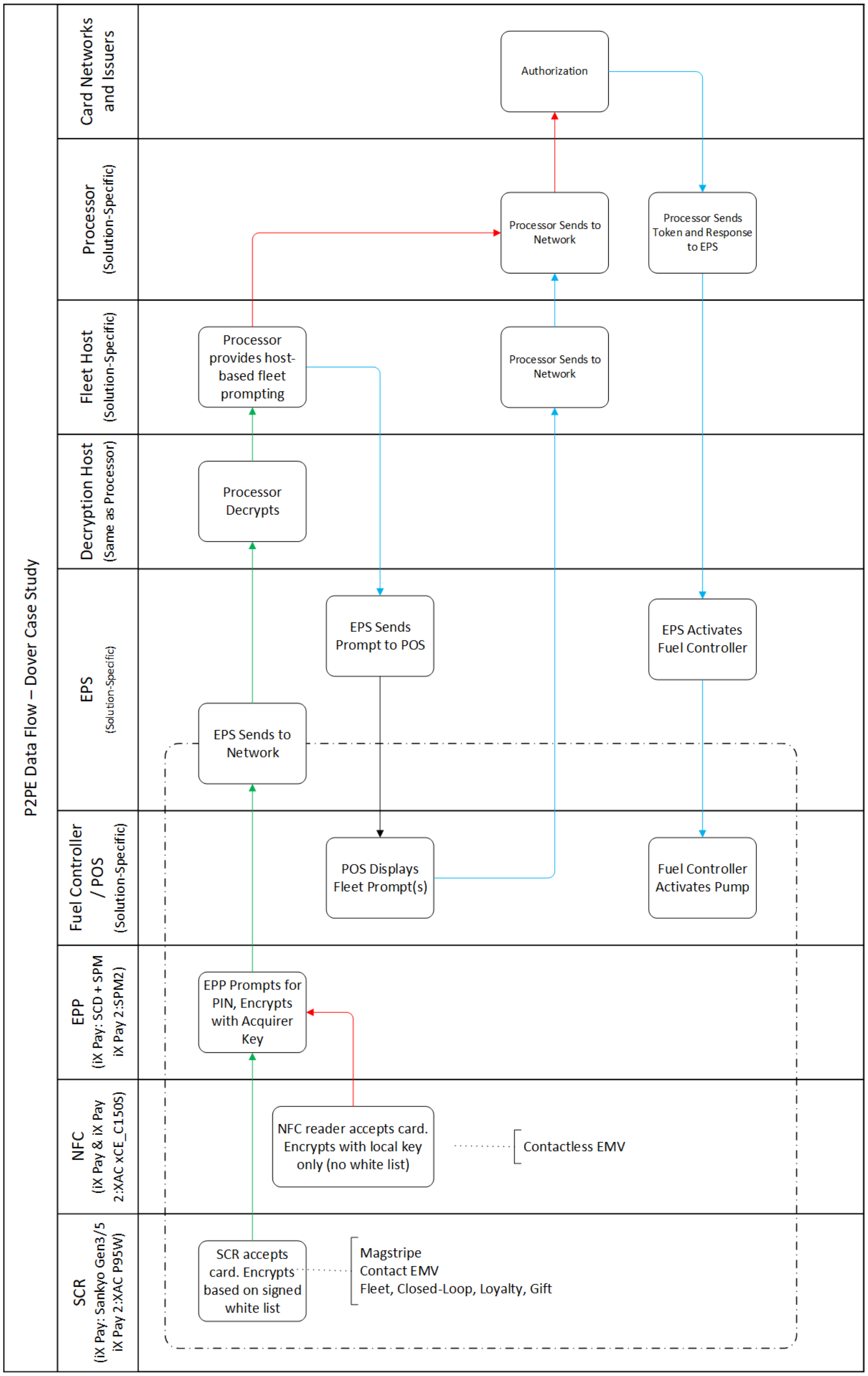

P2PE Data Flow – Dover Case Study
Card Networks and Issuers
Processor (Solution-Specific)
Fleet Host (Solution-Specific)
Decryption Host (Same as Processor)
EPS (Solution-Specific)
Fuel Controller / POS (Solution-Specific)
EPP (iX Pay: SCD + SPM iX Pay 2:SPM2)
NFC (iX Pay & iX Pay 2:XAC xCE_C150S)
SCR (iX Pay: Sankyo Gen3/5 iX Pay 2:XAC P95W)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
Processor provides host-based fleet prompting
Processor Sends to Network
Processor Decrypts
EPS Sends Prompt to POS
EPS Activates Fuel Controller
EPS Sends to Network
POS Displays Fleet Prompt(s)
Fuel Controller Activates Pump
EPP Prompts for PIN, Encrypts with Acquirer Key
NFC reader accepts card. Encrypts with local key only (no white list)
Contactless EMV
SCR accepts card. Encrypts based on signed white list
Magstripe
Contact EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 4B – Dover Fueling Solutions Data Flow for Use in P2PE Solution

5.3 Impacts by Card Type

This solution manages each of the following card use cases as described below:

5.3.1 Consumer Cards

iX Pay: PCI-branded cards are encrypted within the iX Pay SPM (EPP) in SRED using a unique session key derived using the same BDK from the SPM (EPP), and re-encrypted by an SCD device within the UPT before transmission to the POS.

iX Pay 2: PCI-branded cards are encrypted within the iX Pay 2 SPM2 (EPP) in SRED, within the UPT, before being sent in its original encrypted form to the POS.

Non-PCI-branded consumer cards will be encrypted unless they are contained in the BIN whitelist.

5.3.2 Fleet

Through the use of a BIN whitelist, the iX Pay series can optionally ensure that all PCI-branded fleet cards are encrypted. In this configuration, branded fleet cards which require prompting must use host-based messaging to route prompts back to the AFD post-decryption. This setting is contingent upon implementation, and PreEdit or Host-Based Dynamic prompting is contingent upon support by the processor and controller.

Non-PCI fleet cards are generally whitelisted, leaving these cards unencrypted, and allowing prompting to occur using existing, standard methods within the AFD.

Where fleet prompting is performed based on IIN/BIN alone, these flows are unaffected by P2PE whitelist, as the 6-digit BIN remains in clear-text even for encrypted transactions.

5.4 Security and Compliance Impacts

The iX Pay UPT includes EPP, SCR, and an SCD that performs re-encryption within the security boundary of the UPT. This configuration provides secure encryption within the tamper-resistant UPT, but due to the use of a unique session key derived from the same BDK within the SPM (EPP) for the encryption between SPM (EPP) and SCR (SRED) in this configuration, it is not currently compatible with the PCI P2PE v2.0 or v3.0 standards.

The iX Pay 2 UPT leverages SRED-encryption with a unique key per device, making it suitable for use in a PCI P2PE solution.

5.4.1 Security Impact

Use of the iX Pay EPP as a tamper-responsive/tamper-evidence secure cryptography device for all solution provider key storage, and data encryption/decryption/translation may provide risk reduction by ensuring that this sensitive security operation is protected from eavesdropping or manipulation of keys.

5.4.2 PCI P2PE Compliance Impacts

The iX Pay is not suitable for use in a PCI P2PE solution. Since in the SPM (EPP) the session key between the SPM (EPP) and SCR derived from the same BDK of the SPP (EPP) (violates 6E-4.1) and there is no classification for PCI POI certification for SCD, the iX Pay solution will not be suitable for PCI P2PE validated solution.

The iX Pay 2 solution does not employ an EPP loaded with a static key, nor does it perform onsite decryption, and thus may be suitable for use in a PCI P2PE solution. iX Pay 2 UPT has a PCI P2PE validated solution deployed with DFS's OASE decryption solution for the EMEA market. There is a validated PCI P2PE software application on iX Pay 2 that is deployed in EMEA market as well.

5.4.3 PCI DSS Compliance Impacts

Merchants that implement encryption via the iX Pay or iX Pay 2 outside a listed PCI P2PE solution should consult with their QSA and/or acquirer to determine the confirm the strong cryptography, segregation of key management, and the impacts of these on the applicability of PCI DSS for in-scope systems.

Although no current PCI-listed P2PE solution for North America has DFS's OASE implementation utilizing the iX Pay 2, in the event that this UPT POI is implemented as part of a PCI P2PE solution in the future, merchants that properly implement according to the solution provider's requirements may expect to receive PCI DSS scope reduction commensurate with the P2PE program, which may include the usage of the SAQ P2PE for submission of annual assessment.

6 Case Study - Gilbarco FlexPay II and FlexPay IV AFDs

Gilbarco FlexPay devices are PCI OEM PEDs that receive card data via secure channel and perform processor card data encryption within the PED.

6.1 Devices, Systems, and Service Providers

This case study relates to the configuration consisting of the following technologies. Additional solution-specific technologies or vendors may also be present:

OPT POIs Supported

FlexPay II

- **PED:** FlexPay II CDU
- **SCR:** Sankyo or MagTek MSR, ICCR
- **NFC:** Verifone UX410
- **EPP:** Cryptera

FlexPay IV

- **PED:** FlexPay IV UPM
- **SCR:** Verifone UX300
- **NFC:** Verifone UX400
- **EPP:** Integrated with PED

Pumps Supported:

Gilbarco: Various
Wayne: Various

POS/EPS: Solution-Specific

Decryption Entity: Solution-Specific

Acquirer/Processor: Solution-Specific

6.2 Data Flow Diagrams

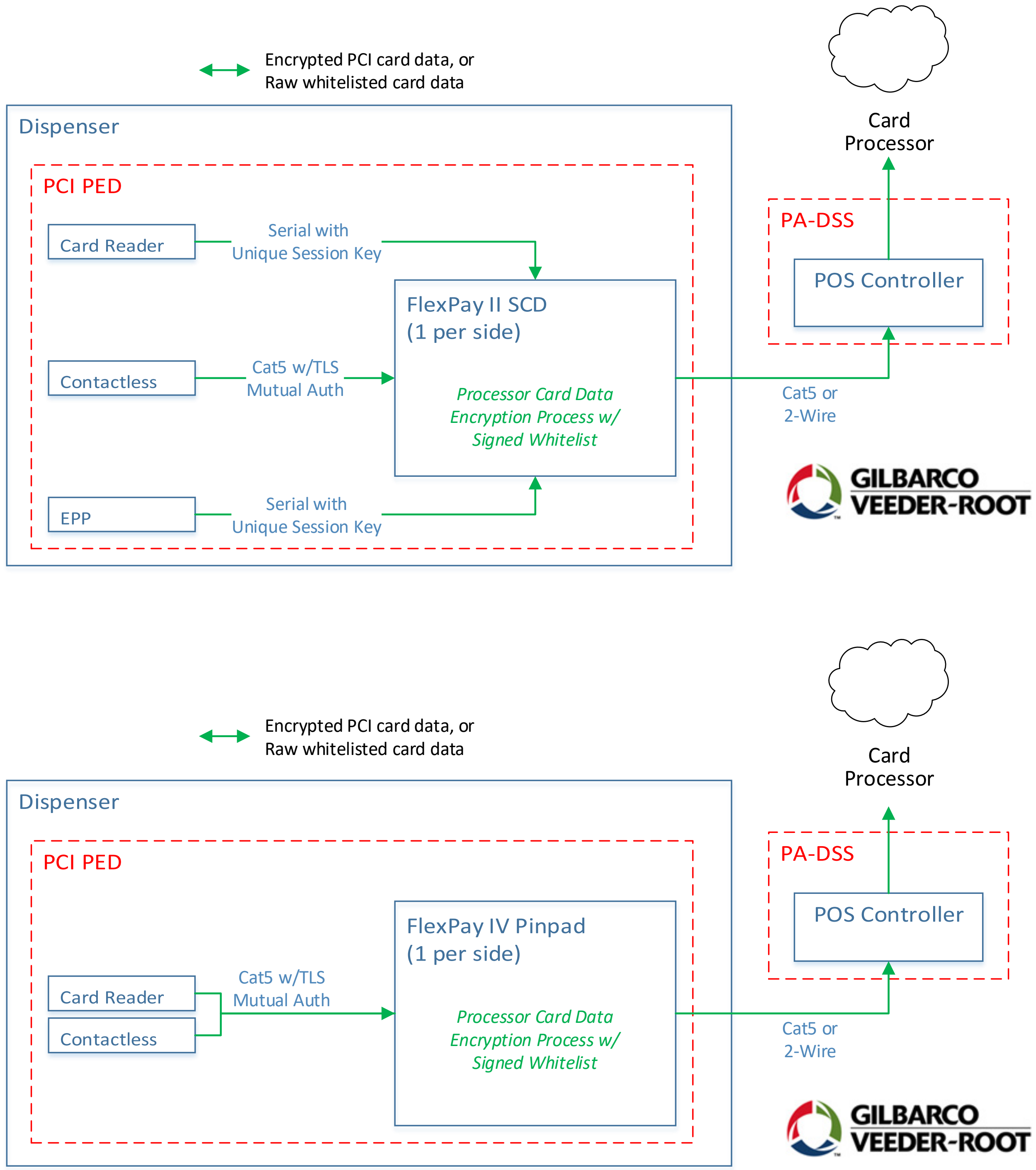


Figure 5A – Gilbarco-Supplied Architecture Diagram

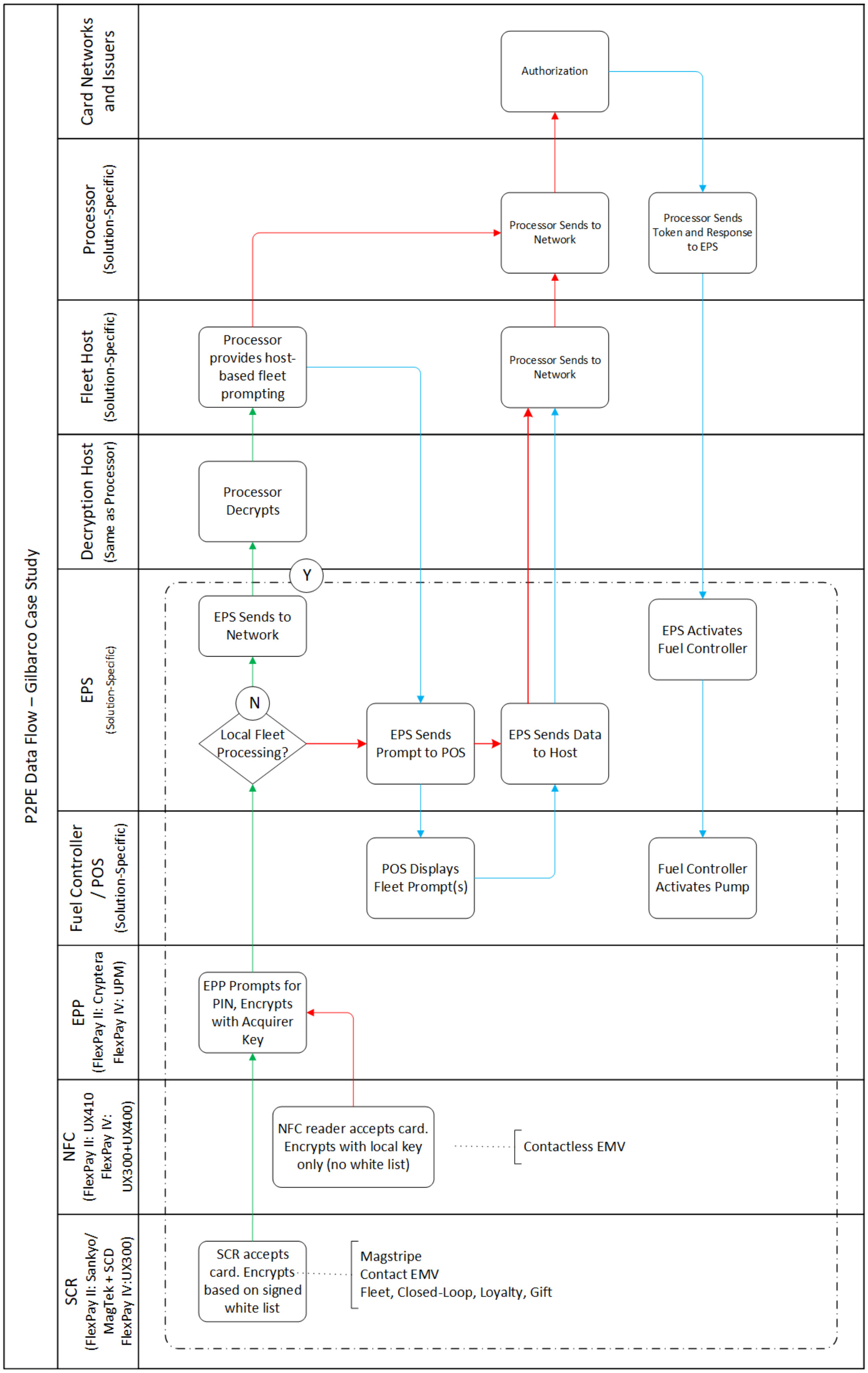

P2PE Data Flow – Gilbarco Case Study
Card Networks and Issuers
Processor (Solution-Specific)
Fleet Host (Solution-Specific)
Decryption Host (Same as Processor)
EPS (Solution-Specific)
Fuel Controller / POS (Solution-Specific)
EPP (FlexPay II: Cryptera FlexPay IV: UPM)
NFC (FlexPay II: UX410 FlexPay IV: UX300+UX400)
SCR (FlexPay II: Sankyo/ MagTek + SCD FlexPay IV:UX300)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
Processor provides host-based fleet prompting
Processor Sends to Network
Processor Decrypts
Y
EPS Sends to Network
EPS Activates Fuel Controller
N
Local Fleet Processing?
EPS Sends Prompt to POS
EPS Sends Data to Host
POS Displays Fleet Prompt(s)
Fuel Controller Activates Pump
EPP Prompts for PIN, Encrypts with Acquirer Key
NFC reader accepts card. Encrypts with local key only (no white list)
Contactless EMV
SCR accepts card. Encrypts based on signed white list
Magstripe
Contact EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 5B – Gilbarco Data Flow for Use in P2PE Solution

6.3 Impacts by Card Type

For all card types the card reader delivers card data to FlexPay PED via SRED-compliant encrypted channel. FlexPay PED encrypts the card data according to the processor-specific formatting and method.

The FlexPay PED accepts a properly-signed whitelist which provides rules for BIN encryption schemes.

6.3.1 Non-ISO Cards

Current FlexPay PED P2PE implementation does not allow output of non-ISO cards. This is currently being reviewed for potential enhancements to support identified customer flexibility needs.

6.4 Security and Compliance Impacts

FlexPay PED implements a plug-in architecture that allows multiple types of card data encryption schemes. Each P2PE plugin implements its own rules for key and resource management (using the PED's security functions). All P2PE plugins are submitted for PCI PTS delta approval, ensuring that all software-based logic is included within the PTS firmware approval, as opposed to P2PE application validation.

6.4.1 Security Impact

The encryption of account data within the PED can provide end-to-end encryption for account data, protecting card information from eavesdropping within the merchant environment. The tamper-responsive mechanisms of the FlexPay devices provide additional protection from intrusion or compromise of keys or account data.

6.4.2 P2PE Compliance Impacts

While the FlexPay PED provides account data security, it has not yet been validated within a P2PE solution. No known issues exist that would prevent the FlexPay II or FlexPay IV from being used within such a solution, although it is notable that local fleet prompting would not be available for cards issued by the PCI card brands.

6.4.3 PCI DSS Compliance Impacts

Since the FlexPay solutions have not been validated to PCI-P2PE, merchants using any such solution should check with their acquirer for the appropriate SAQ or PCI DSS scope impact for a corresponding ROC, based on the protections provided by these devices and encryption mechanisms.

7 Case Study – Invenco – Automated Fuel Dispenser

Invenco offers a range of pay-at-pump (AFD) terminals that are retrofit into existing as well as new headless pumps. The Invenco line offers multiple solutions with barcode readers and contactless as standard in all their configurations and is available in a range of capabilities from a 5” touch all-in one terminal that fits pumps in the market to a family of 8”, 12”, and 15” modular touch screen options designed for the ATM style appearance.

The P2PE framework that is available in all Invenco terminals provides an extensive plug-in design which can support a unique P2PE configuration per BIN range – this supports an implementation where every type of card could use its own set of keys and its own P2PE encryption algorithm. This design allows retailers to individually manage requirements for Visa, Mastercard, Amex, Discover, Union Pay, JCB, fleet, loyalty, and other proprietary cards to potentially avoid impacts from requirement changes in the future. All of these configurations and keys are managed through a centralized PCI DSS certified cloud application. When combined with other PCIcertified P2PE card host elements, these products can deliver a PCI-validated P2PE offering. Today, the Invenco terminals support 8 different P2PE implementations, and that number continues to grow.

Invenco terminals are installed using pre-assembled retrofit assemblies for the particular pump type in which they will be installed. This means that they are pre-wired or in the case of the all-in-one, pre-mounted to fit the particular pump. Devices are pre-staged for a particular customer and remaining configuration can be deployed via the Invenco Cloud Services application. This cloud configuration can include various keys, plug-ins, and other configurations for the terminal to talk with the host. The design of this process streamlines the installation and can minimize the complexity of installation and ongoing support of the product.

7.1 Devices, Systems, and Service Providers

POI:

- **UPT:** Invenco G6-300 OPT
- **UPT:** Invenco G7-100-12 OPT
- **UPT:** Invenco G7-100-15 OPT
- **UPT:** Invenco G7-100-8 OPT

Pumps Supported:

Gilbarco: Advantage, Encore 300/500, Encore 500S/700S

Wayne: Vista 0/1/2/3/4, Ovation 1 & 2, Helix

Tokheim: Premier B/C

Other: Tatsuno, European variants

POS/EPS: Various US / UK / Malaysia / NZ POS-EPS systems
Encryption Schemes: TransArmor RSA, Various TDES variants, Standard RSA, AES, Proprietary
Decryption Management: First Data TransArmor, Other proprietary host variants
Processor: First Data, Worldpay, UK processor, MY processor, NZ Paymark
P2PE Solutions: Several P2PE solutions using Invenco devices are available in Europe and Asia, however no North American PCI-listed solutions exist to support these devices.

7.2 Data Flow Diagrams

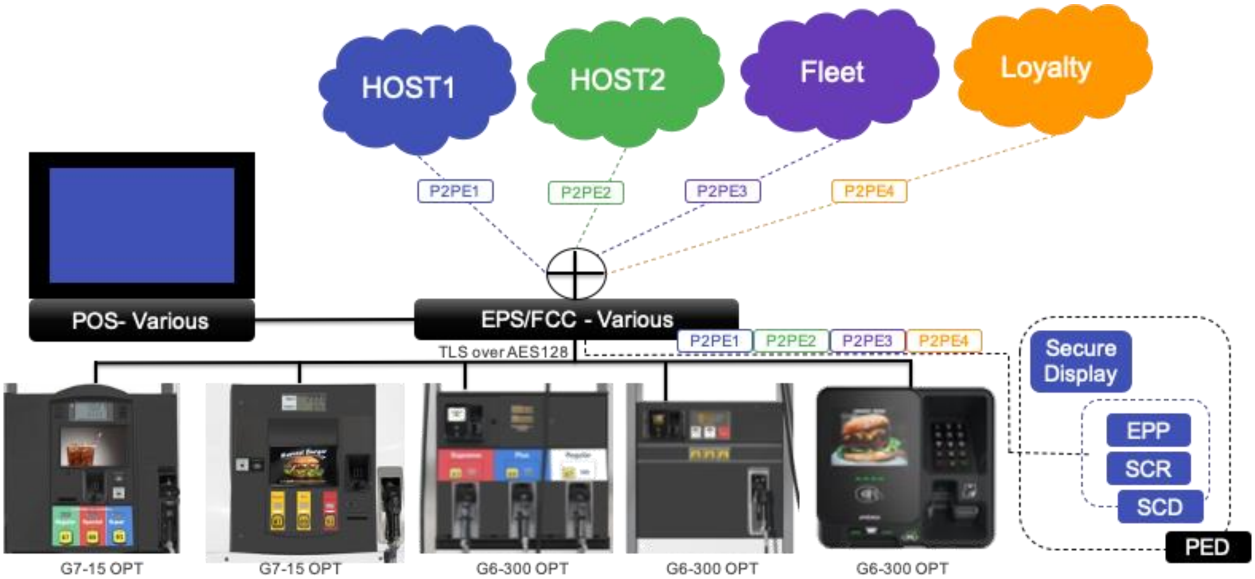


Figure 6A – Invenco-Supplied Architecture Diagram

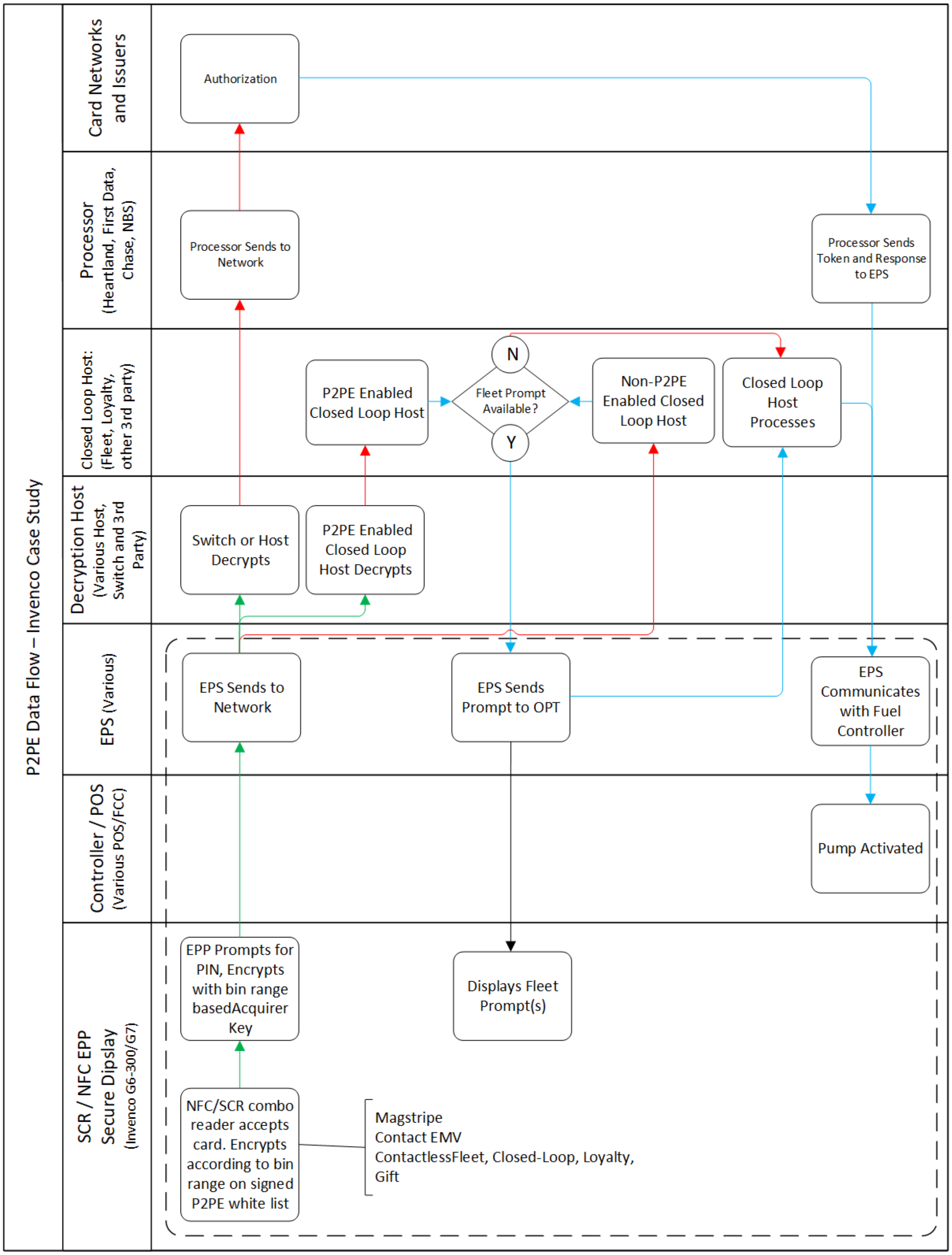

P2PE Data Flow – Invenco Case Study
Card Networks and Issuers
Processor (Heartland, First Data, Chase, NBS)
Closed Loop Host: (Fleet, Loyalty, other 3rd party)
Decryption Host (Various Host, Switch and 3rd Party)
EPS (Various)
Controller / POS (Various POS/FCC)
SCR / NFC EPP Secure Dipslay (Invenco G6-300/G7)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
P2PE Enabled Closed Loop Host
N
Fleet Prompt Available?
Y
Non-P2PE Enabled Closed Loop Host
Closed Loop Host Processes
Switch or Host Decrypts
P2PE Enabled Closed Loop Host Decrypts
EPS Sends to Network
EPS Sends Prompt to OPT
EPS Communicates with Fuel Controller
Pump Activated
EPP Prompts for PIN, Encrypts with bin range basedAcquirer Key
Displays Fleet Prompt(s)
NFC/SCR combo reader accepts card. Encrypts according to bin range on signed P2PE white list
Magstripe
Contact EMV
ContactlessFleet, Closed-Loop, Loyalty, Gift

Figure 6B – Invenco Data Flow for Use in P2PE Solutions

7.3 Impacts by Card Type

The Invenco architecture is unique in its design. Its implementation of a secured, downloadable card table allows the P2PE system to be quite flexible. The solution includes the ability to customize the masking and leverage the key management and encryption methodology by BIN range. Also, each of these keys and key slots may be managed from the cloud, so it is not necessary to send Invenco units to a secure room or visit the terminals at the site to activate their P2PE capabilities.

This solution manages each of the following card use cases as described below:

7.3.1 Consumer Cards

The Invenco terminals support the use of cryptographically authentication BIN range configuration to determine whether or not the card data should be encrypted, how it should be encrypted, how it should be masked, and which keys to use in the process. PCI-branded consumer cards use the keys and the encryption methodology associated with the next step in the encryption/decryption process which could be a P2PE solution or in some cases all the way to the host processor (E2EE). All non-PCI cards can be encrypted with their own key/scheme or left unencrypted (proprietary loyalty, etc.) as is needed for in-store and above store processing.

7.3.2 Fleet

Closed loop, proprietary, loyalty and fleet cards (PCI and non-PCI) have all the same flexibilities for processing available to them by BIN range as the PCI cards described above. This means through the configuration of the card table and P2PE plug-ins, that each fleet card can have its own masking technique, key management, and encryption algorithm (including none of the above) to meet the processing requirements of various EPS/host combinations.

7.4 Security and Compliance Impacts

All Invenco devices are PCI-PTS certified devices and are constantly being updated to the latest standard. Most of the devices listed above are PTSPTS v5. The ones that are PTSPTS v4 are currently under evaluation for an update to PTSPTS v5. Invenco engineers all their devices and security mechanisms from the ground up (as opposed to use of third-party equipment). Invenco works with organizations like PCI, EMVCo and host providers to provide compliant solutions.

7.4.1 Security Impact

Implementations that use the Invenco P2PE framework ensure that card data is encrypted in an SRED security zone using DUKPT and sometimes proprietary host--

provided keys, all of which are enclosed in a tamper responsive security area. These keys are only known to the P2PE endpoint and host providers and are managed under a PKI infrastructure. Leveraging this framework, Invenco is able to provide a flexible, cloud-managed card data security framework that works with EPS and card host providers around the world.

In addition, most implementations are using an AES-128 line-level encryption on all outdoor lines and a TLS--secured connection between terminal and store applications. This layered approach to encryption provides additional security for keeping data safe.

7.4.2 PCI P2PE Compliance Impacts

Invenco is pursuing component-based PCI P2PE certifications for its applications and applicable components, and in conjunction with various P2PE providers with various capabilities for secured unattended payments, in use all over the world. Invenco provides a P2PE framework that helps retailers manage the costs associated with using keys from distribution hosts rather than in physical secure rooms, updating keys in the event of a breach, and updating algorithms (AES, ECC, etc.) for the future. Invenco is also working with PCI SSC to request inclusion of these approaches in the next PCI P2PE standard so that retailers can have both a mechanism to take systems out of PCI scope and assist in managing the updates to the system in a secure, compliant manner.

7.4.3 PCI DSS Compliance Impacts

A goal of having a P2PE solution is to allow retailers to provide the paperwork to an auditor that takes a majority of their systems out of PCI scope. In New Zealand for example, the processor has taken its own position that site systems are out of scope for PCI if they follow a particular process and architecture for processing and data encryption (even though this is not a PCI P2PE certified solution). Retailers should balance their needs/costs related to the PCI DSS audits over the costs of a certified P2PE infrastructure. In reality, a well-prepared PCI DSS assessment document that demonstrates what a retailer has done to protect card data (and P2PE is a great complement to that) can dramatically streamline the PCI DSS audit process.

8 Case Study – NCR OPTIC 12 – Automated Fuel Dispenser

NCR OPTIC 12 pay-at-pump terminal offers a modular, self-service solution that comes EMV ready standard with 12in touch screen, contactless reader (including mobile phones), 2D barcode scanner and mag stripe reader. OPTIC 12 provide retrofit options for most pump brands.

8.1 Devices, Systems, and Service Providers

POI:

- **UPT:** Invenco G7/G6-200

Pumps Supported: Encore 300 (modifications required), Encore 500, Encore 500S, Encore 700S; Dover Wayne Ovation, Ovation 2, Helix
POS/EPS: NCR EPS
Encryption Schemes: TransArmor RSA
Decryption Management: First Data TransArmor
Processor: First Data

8.2 Data Flow Diagrams

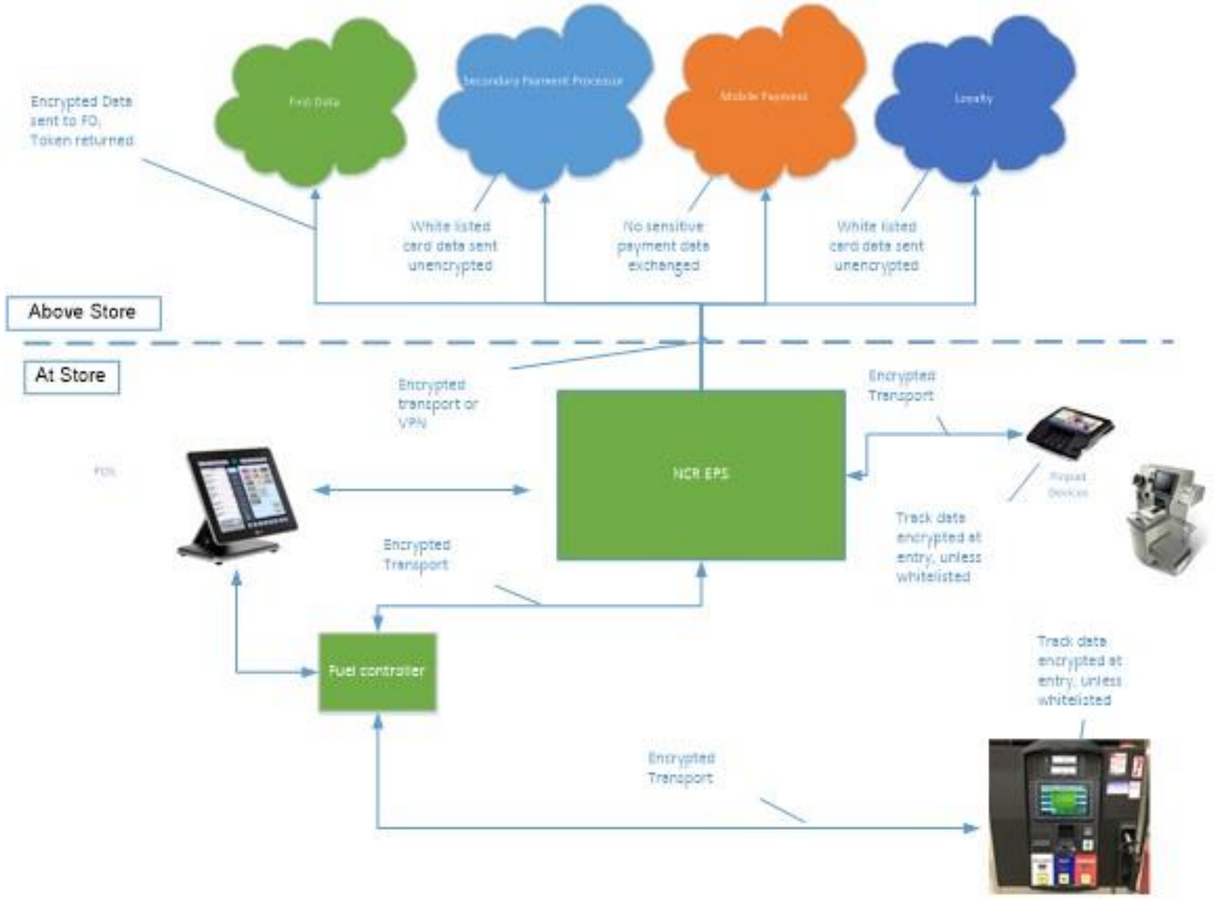

First Data
Secondary Payment Processor
Mobile Payment
Loyalty
Encrypted Data sent to FD, Token returned
White listed card data sent unencrypted
No sensitive payment data exchanged
White listed card data sent unencrypted
Above Store
At Store
Encrypted transport or VPN
Encrypted Transport
NCR EPS
POS
Pinpad Devices
Track data encrypted at entry, unless whitelisted
Encrypted Transport
Fuel controller
Track data encrypted at entry, unless whitelisted
Encrypted Transport

Figure 7A – NCR-Supplied Architecture Diagram

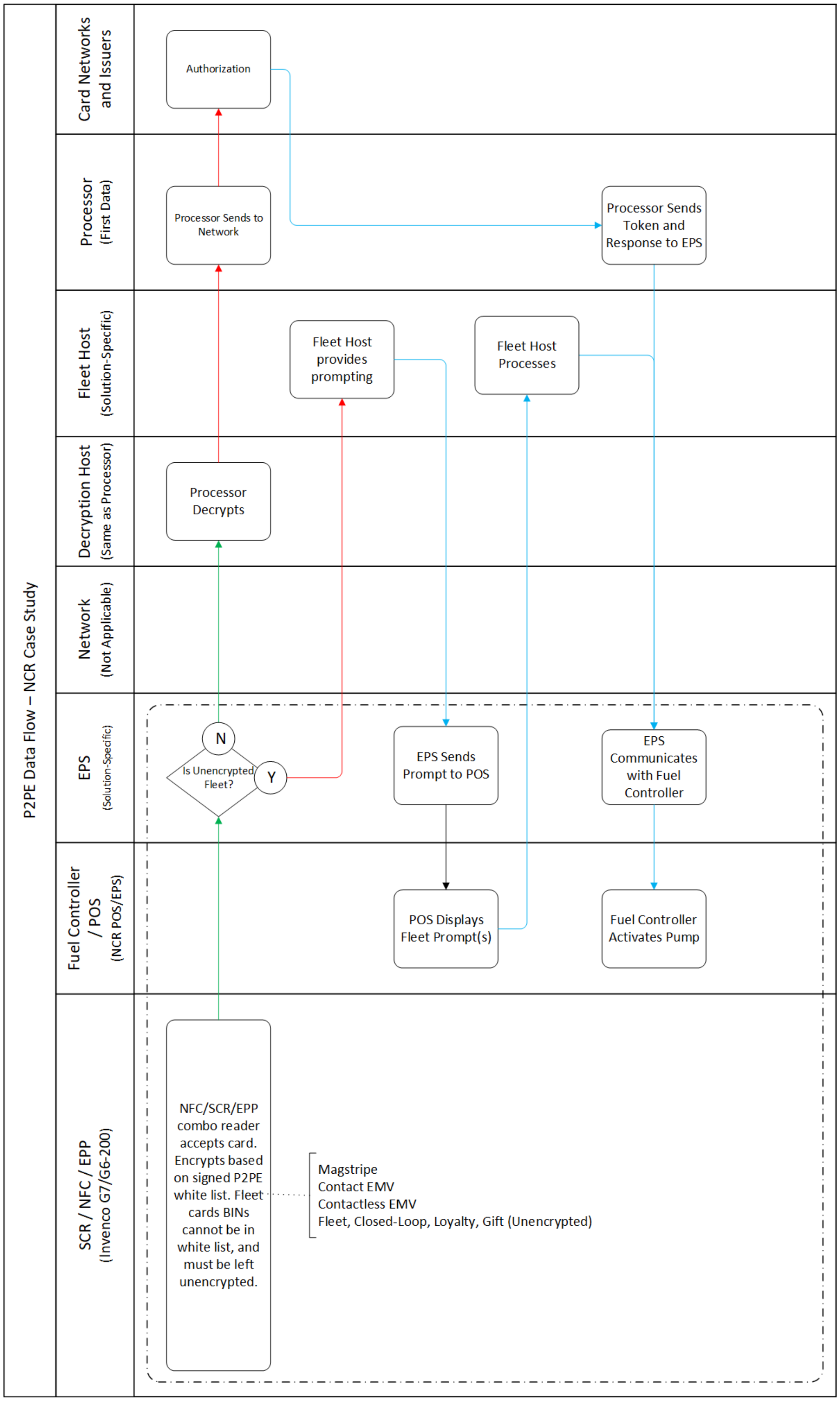

P2PE Data Flow – NCR Case Study
Card Networks and Issuers
Processor (First Data)
Fleet Host (Solution-Specific)
Decryption Host (Same as Processor)
Network (Not Applicable)
EPS (Solution-Specific)
Fuel Controller / POS (NCR POS/EPS)
SCR / NFC / EPP (Invenco G7/G6-200)
Authorization
Processor Sends to Network
Processor Sends Token and Response to EPS
Fleet Host provides prompting
Fleet Host Processes
Processor Decrypts
N
Is Unencrypted Fleet?
Y
EPS Sends Prompt to POS
EPS Communicates with Fuel Controller
POS Displays Fleet Prompt(s)
Fuel Controller Activates Pump
NFC/SCR/EPP combo reader accepts card. Encrypts based on signed P2PE white list. Fleet cards BINs cannot be in white list, and must be left unencrypted.
Magstripe
Contact EMV
Contactless EMV
Fleet, Closed-Loop, Loyalty, Gift (Unencrypted)

Figure 7B – NCR Data Flow for Use in P2PE Solutions

8.3 Impacts by Card Type

This solution manages each of the following card use cases as described below:

8.3.1 Consumer Cards

The NCR Optic UPT supports the use of cryptographically authenticated BIN whitelist to determine which cards may be left unencrypted. PCI-branded consumer cards should remain encrypted and processed by the TransArmor solution. Where non-PCI-branded consumer cards are intended to be left unencrypted, these BINs must be identified within the whitelist and routed to alternate host for processing.

8.3.2 Fleet

Host-based fleet prompting for non-PCI-branded fleet cards may be supported by TransArmor processing host or may be passed to a separate fleet card processing host. In either case, these cards may be listed in the BIN exclusion list, left unencrypted and routed accordingly by the EPS.

BIN-based fleet prompting can be supported directly within the Optic solution since BIN is left unencrypted by TransArmor for all card types.

Fleet prompting for PCI-branded cards that rely upon discretionary data or track equivalent data (EMV) does not require leaving these PCI-branded data unencrypted in many cases. Optic is able to identify most common fleet cards at point of entry and allow exposure of the required discretionary data for fleet prompting.

8.4 Security and Compliance Impacts

The TransArmor RSA solution provides key management and encryption of account data for decryption and processing by the First Data TransArmor host. This methodology can improve the security of the merchant environment by securely exchanging signed keys for use in supported terminals, and encryption using strong cryptography.

8.4.1 Security Impact

RSA encryption provides encryption using 2048-bit RSA keys. The public key for the transaction resides on the NCR POI, and may be periodically rotated according to TransArmor configuration. Cardholder data encryption is non-format preserving. Proper implementation of the NCR Optic solution supports secure key exchange and encryption, using strong cryptography, and thus can improve the overall security of account data in the merchant environment.

8.4.2 PCI P2PE Compliance Impacts

FirstData currently has several TransArmor solutions validated and listed as PCI P2PE solutions. However, at the time of publication, these NCR/Invenco devices, configuration, and solution management are not yet validated to the PCI P2PE program. The use of SRED by the NCR/Invenco POI and use of RSA-2048 encryption could potentially support P2PE validation in the future.

8.4.3 PCI DSS Compliance Impacts

Merchants should check with their acquirer to confirm scope and applicability of PCI DSS controls afforded through the use of these acquirer-based solutions.

9 Case Study – Verifone Commander P2PE solution for indoor POS and outdoor AFDs

Verifone Commander is a site controller solution supporting attended POS operations indoors and unattended AFD operations outdoors. The P2PE solution available on Commander is device and acquirer agnostic. The solution provides decryption services in the Verifone Cloud ensuring card data is never in the clear within the merchant environment.   This solution's initial implementation utilizes Verifone's format-preserving VSP Derived Key (VSPDK) encryption scheme which is widely used in retail environments. Currently, implementations of the VSPDK are available for indoor PIN Pads and outdoor AFD POIs from Gilbarco and Wayne. The solution is not currently a PCI-validated P2PE solution, but a PCI validate-able AES DUKPT P2PE solution is planned in a later phase.

9.1 Devices, Systems, and Service Providers

The Verifone VSPDK P2PE solution supports multiple indoor PIN Pads and a number of widely used outdoor devices.

IPT POIs Supported

- MX9xx
- M400 (or any Engage Product)

Pumps Supported

- Gilbarco (via Verifone's VCL libraries resident on the device)
- Wayne (via Verifone's VCL libraries resident on the device)

OPT POIs Supported: Any supported OPT. The Verifone Commander currently supports Gilbarco and Wayne. Support is underway for Bennett and Invenco utilizing the new Conexxus Forecourt Payment Standard.

Encryption Management: Device-dependent. Verifone performs many encryption management operations, including managing the content and signing of files for indoor devices. Verifone also manages the contents of any files for outdoor devices, but the applicable vendor must sign the files required for the outdoor devices. Verifone works with the merchant sites to ensure each device is properly configured.

Encryption Scheme: Verifone VSP Derived Key Format-Preserving Encryption

Decryption Management: Verifone Cloud Services

9.2 Data Flow Diagrams

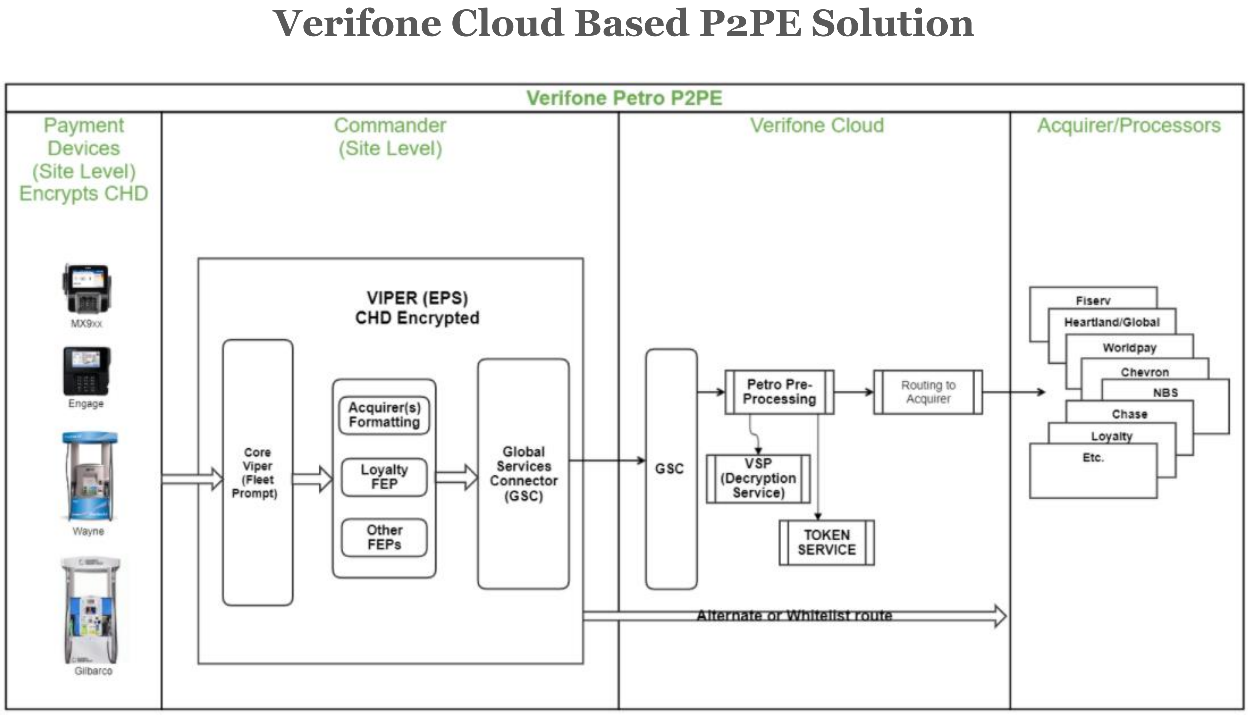


Figure 8A – Verifone-Supplied Architecture Diagram

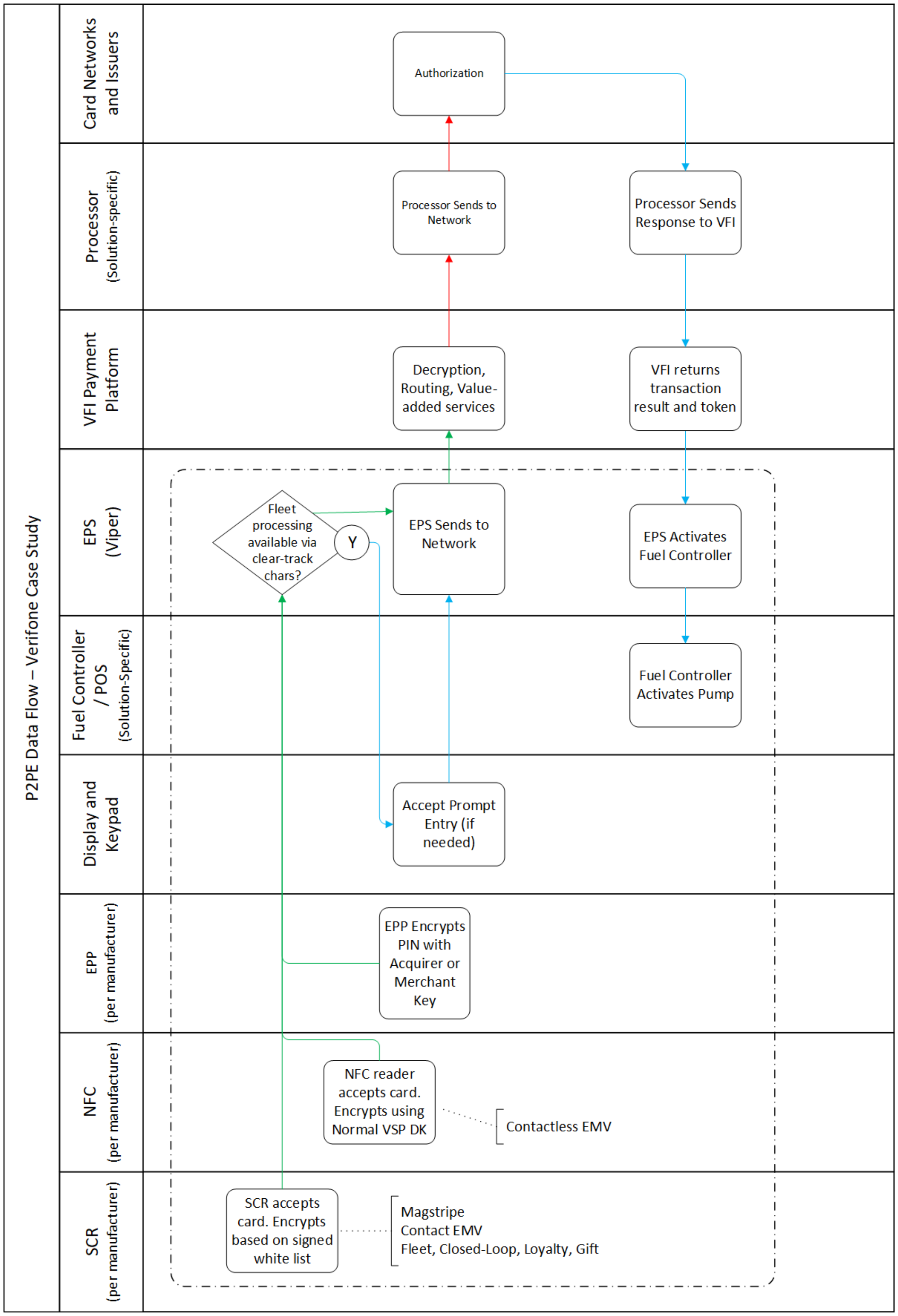

P2PE Data Flow – Verifone Case Study
Card Networks and Issuers
Processor (Solution-specific)
VFI Payment Platform
EPS (Viper)
Fuel Controller / POS (Solution-Specific)
Display and Keypad
EPP (per manufacturer)
NFC (per manufacturer)
SCR (per manufacturer)
Authorization
Processor Sends to Network
Processor Sends Response to VFI
Decryption, Routing, Value-added services
VFI returns transaction result and token
Fleet processing available via clear-track chars?
Y
EPS Sends to Network
EPS Activates Fuel Controller
Fuel Controller Activates Pump
Accept Prompt Entry (if needed)
EPP Encrypts PIN with Acquirer or Merchant Key
NFC reader accepts card. Encrypts using Normal VSP DK
Contactless EMV
SCR accepts card. Encrypts based on signed white list
Magstripe
Contact EMV
Fleet, Closed-Loop, Loyalty, Gift

Figure 8B – Verifone Data Flow for Use in P2PE Solutions

9.3 Impacts by card type

This solution manages each of the following card use cases as described below:

9.3.1 Consumer Cards

PCI-branded cards are encrypted within each device using the VCL libraries prior to being passed to the device controller. VSPDK supports the use of a BIN whitelist, the contents of which is managed by Verifone as the site payment controller vender. Each PED equipment provider (e.g., Verifone, Wayne, Gilbarco) must perform the appropriate signing as required.

Any card not in the BIN whitelist will be encrypted.

9.3.2 Fleet

Host-based fleet processing where the prompts come from the issuer host (e.g., OTR fleet) is not impacted, since the card data is fully decrypted when it reaches the issuer.

Card-based fleet processing is managed via the VSPDK BIN whitelist file. The whitelist contains syntax that allows the VSPDK encryption to leave fleet data in the clear. The remaining data is encrypted using the normal VSPDK format-preserving encryption.

Card-driven, “Host-based” prompting, where the cloud returns fleet prompts after decrypting the card data is also a potential solution for fleet cards in the future. This operation is not yet implemented but is on the development roadmap.

Recent EMV fleet offerings by Visa Fleet and WEX utilize the Conexxus standard that provides non-sensitive EMV data tags for the prompt and product restriction fleet data. Mastercard Fleet and Voyager follow a proprietary specification, but also provide fleet data in non-sensitive EMV data tags. Current support for the EMV data tags is currently (Q1 2021) inconsistent among acquirers, but when fully supported will alleviate the need to provide whitelist exclusions for EMV fleet cards.

9.4 Security and Compliance Impacts

Since the Verifone solution supports many card data acquisition devices, a blanket statement about device capability is not possible. The solution does ensure that all card data, while present in the merchant’s environment, is encrypted subject to limitations due to BIN whitelisting and fleet prompting requirements. The card data is never decrypted within the merchant environment, thereby providing protection from network-based attacks, malware, or breaches in physical security within the merchant environment.

9.4.1 Security Impact

The solution uses Verifone's VSPDK format-preserving encryption. The encryption functionality is supported by numerous POI devices via included VCL libraries. The key setup and management are supported via specified messaging between the POI, Commander and the Verifone Cloud.

Properly configured, the VSPDK ensures encryption of all cardholder data, reducing risk and improving security of these data in the fuel dispenser.

As with any card present solution external skimmers may still be a threat as they may access account data prior to encryption by the POI.

9.4.2 PCI P2PE Compliance Impacts

The current Commander P2PE solution using VSPDK is not a PCI-Validated P2PE solution. Roadmap plans include adding an AES DUKPT encryption scheme that, when supported by all the applicable devices, could be validated as part of a PCI-P2PE solution.

9.4.3 PCI DSS Compliance Impacts

Merchants that implement Commander's P2PE encryption via Verifone's VSPDK Format-Preserving Encryption should consult with their QSA to determine the impacts of the cryptography and key management on the applicability of PCI DSS for in-scope systems.

As the AES DUKPT rollout is complete and a PCI-validated P2PE solution becomes available, merchants that properly implement according to the solution provider's requirements may expect to receive PCI DSS control reduction commensurate with the specific P2PE program. Furthermore, merchants that implement Verifone devices in other PCI-validated P2PE solutions will receive similar scope reduction.

10 Conclusion

The fuel retail industry in North America continues to see cardholder data compromise due to unencrypted account data in the forecourt. As an industry, and as individual merchants, there is a vested interest in migrating to point-to-point encryption as a means of reducing exposure of clear-text account data in this vulnerable environment.

The hardware, systems, and service providers identified in these case studies do not represent all available options, and each has unique implementation, security, and compliance impacts. Nonetheless, each demonstrates the availability of terminal-based encryption in the fuel dispenser which may improve security in the forecourt and provide a starting place for conversations with merchant acquirers, POS, EPS, decryption, and third-party solution providers for effective research and implementation of point-to-point encryption.

A. Appendix – Common Considerations

A.1 Common Terminal Encryption Logic

When considering device encryption, it is important to consider all cards which will be accepted via the POI device interface, not just payment cards. The following special cases should be considered:

A.1.1 Local Cards

Any local payment cards that should be left unencrypted must be added to the BIN exclusion whitelist in order to be left unencrypted. These could include closed-loop, gift card, stored value, or other cards which do not carry the Visa, Mastercard, American Express, or JCB logos, and are intended for processing by the POS or other local system as opposed to network authorization.

A.1.2 Loyalty Cards

Cards not used for payments, such as loyalty program cards, will be encrypted if they are not included in the BIN whitelist. For local cards that should not be encrypted and therefore accessible to the POS, these must be added to the BIN exclusion whitelist.

A.1.3 Non-ISO / Non-EMV ICC cards

Cards that are not recognized as ISO/IEC 7813 specific track, or EMV ICC tag formatting (such as one which may be used for employee authentication or driver’s license) will be left unencrypted.

The following table summarizes common behavior by encryption terminals:

Card Type	Test	Encrypted	Not Encrypted	Implementation Notes
ISO/IEC 7813 Magstripe or EMVCo ICC Card	IIN/BIN in Whitelist		✓	Used for non-PCI branded cards or cards that the decryption host cannot process. Leaving PCI-branded card unencrypted can impact merchant compliance and increase risk.
	IIN/BIN Not in Whitelist	✓		Generally used for PCI cards and any other BINs that the decryption host is able to process.
Non-ISO/EMV Card	All		Usually	Many SCR devices will either leave non-ISO magstripe/non-EMV ICC cards unencrypted, however some may generate an error. Check with hardware provider to confirm.

B.Informative References

Payment Card Industry Security Standards Council (PCI SSC) published list of PCI Point-to-point Encryption (P2PE) solutions: https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Payment Card Industry Security Standards Council (PCI SSC) published list of PCI Personal Identification Number (PIN) Transaction Security (PTS) devices: https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

Payment Card Industry Security Standards Council (PCI SSC) document library, containing the P2PE Glossary, P2PE Standards, and P2PE Program Guides: https://www.pcisecuritystandards.org/document_library